On Behalf of Privacy Principles

GW

Shestack's comments, cline in enrollment in ornia "deplorable." Kay the ABA study will find procedures "consistent we are bound by." Kay 3A committee that rec- study.

examining yet-to-be- hools, will examine a ng Law School Admis- AT) scores, she said. y often are a heavily or, along with a stu- graduate grades. The oposes using a mini- old score" to cull out a ents, then using factors es and undergraduate ose among this pool. the ABA, this would st's disparate impact on

ie ABA group recom- study also accredits law oice 1 carry great ding to an ABA spokes-

lso announced that the haling lawyers around help restore welfare isabled children whose eing cut off under the n legislation signed by year. Programs in the d Virginia al- erway to train volunteer andle these cases, ac- ABA staff member. said that as many as ren now receiving Sup- urity Income benefits of month may lose them. he said, "is a form of children, and the ABA lp them out."

FILE PHOTO

Listening In at the Social Security Office

Callers' Privacy May Be Compromised, Inspector General Says

By Stephen Barr
Washington Post Staff Writer

The Social Security Administration monitors telephone calls to assess the quality of service provided to the public by its employees, but callers often do not know that officials are listening in, the agency's inspector general said yesterday.

The IG questioned whether Social Security has the necessary legal authority for monitoring calls and suggested the agency may compromise the privacy of some callers by improperly recording information on agency forms.

Social Security also has limited or no controls to ensure whether telephone monitoring is used for its intended purposes, the IG said. The monitoring program does not create records or audit trails to show when calls are monitored and the software allows for listening in from any touch-tone telephone outside the Social Security phone system, the IG said.

The agency rejected the inspector general's report as misleading and flawed. "The IG is dead wrong when they say we are violating laws," said Social Security spokesman Phil Gambino. "Telephone monitoring is done appropriately, it's necessary, and we protect the privacy of the American public."

Gambino said Social Security monitors calls handled by trainees and other inexperienced staffers to ensure they provide accurate information to the public. No telephone calls are recorded, he said. Last year, the agency provided services to about 48 million callers.

The IG's office yesterday provided a brief "fact sheet" on a July audit of the telephone eavesdropping system after a representative of the American Federation of Government Employees issued a statement saying the agency's "behavior violates the trust of the American people."

Carol Fehner, the union representative, said some officials listening to phone calls can overhear what is going on in a caller's home or business, even when Social Security representatives put the call on hold.

IG spokeswoman Agapi Doulaveris said her office would not comment on the report, which will be published later this week.

A number of retail and service-oriented corporations monitor phone conversations between employees and customers, and virtually all inform callers that a supervisor may be listening in.

But excerpts of the IG audit report, provided by Fehner, concluded that Social Security "may be subject to legal challenges with respect to whether it has the necessary employees' or public's consent." The IG report said the public's only notification about phone monitoring is a brief statement in agency pamphlets. According to the report, Social Security in 1990 eliminated a prerecorded message on its toll-free 800 number that advised the public that calls may be monitored by a second Social Security official.

"We believe the public has the right to know that their calls are being monitored," the IG report said.

The government-wide regulation for telephone monitoring was abolished last year when Congress approved the Information Technology Management Act, which gave each agency the freedom to fashion its own computer and telephone policies. Given the IG's concerns, Social Security will review some of its policies, Gambino said.

Clinton to Widen Federal Offices' Ban on Smoking

SMOKING, From A1

sons. Officials said yesterday it will be made the focus of the president's weekly radio address Saturday.

"This decision is important symbolically, but it's also important to the health of federal government employees and the people who visit government buildings," said Matthew L. Myers, director of the National Center for Tobacco-Free Kids.

"Such an executive order guarantees an individual's fundamental right to work in an environment free of unhealthy smoke," said Sen. Tom Harkin because 15 agencies already ban smoking. The Pentagon, Health and Human Services Department, Postal Service and Environmental Protection Agency have among the toughest policies.

However, others are not as strict. A survey by Lautenberg's office revealed a patchwork set of rules that vary from department to department. According to administration officials, the Transportation Department has smoking lounges, while the Housing and Urban Development Department permits smoking in some restrooms. Commerce Department workers can smoke in private offices and designated cafeterias, while soldiers, sailors and others can puff away in military-owned restaurants and bars.

Among the most visible changes will be the ban on outside entrances, where many workers escape for a smoke during lunchtime and coffee breaks. An earlier draft of the new policy called

Judge Clears Justice Dept. in Inslaw Case

Associated Press

A federal judge has rejected claims that the Justice Department stole a computer program from a local software contractor, government officials announced yesterday.

The decision, made last week in federal claims court, ends a 10-year legal battle over a program that helps prosecutors keep track of cases and share information. The ruling was issued after a three-week trial.

PRIVACY

that back then she knew practically everybody in the field. "Now, there are many firms out there I've never heard of."

Their goal is to know more about children's preferences than even parents do. Researchers host online chats, where kids are more apt to talk openly about personal matters. They hire toddlers to play with new toys and then watch from behind a two-way mirror, often joined by psychologists. Nickelodeon alone surveys 4,000 children every week in its offices, at schools, over the phone, and on the Internet.

Thanks in part to recent academic studies, marketers now know more than ever about the child psyche. That has helped them translate the urges and obsessions of different age groups into bigger sales. By limiting the number of each new Beanie Baby and announcing on its Web site which dolls it had discontinued, Ty Inc. in Oak Brook, Ill., for example, cashed in on the desire of 7-year-olds to collect. That urge used to be satisfied by sea shells or baseball cards, back before the latter became an investment opportunity.

BACKLASH? At the same time, the new research has allowed some companies to shatter long-held assumptions about kids' behavior—such as the belief that female images work with girls but alienate boys. Nickelodeon discovered that kids were changing and didn't hesitate to launch a series of live-action shows with girls as the protagonists. One, *The Secret World of Alex Mack*, now has an audience that is 53% male.

Some of the new kid marketing draws on more troubling trends. It's no secret that images of sexuality and other forbidden pursuits appeal to many teenagers. And marketers, fighting to be noticed, are increasingly calling upon such symbols. Think about the current controversy over "heroin chic" images in fashion magazines. Or last year's Calvin Klein campaign that mimicked cheesy child pornography videos. That may have been the most egregious example of sexualizing children in order to sell to them, but it's not unique.

In fact, there are already signs of a backlash against the constant marketing assault facing kids. In Massachusetts, the Boston Children's Museum is running an exhibit that teaches children to understand commercials by allowing them to experiment with lighting and backdrops to change the look of an object. The purpose, says the museum's director of cultural programs, Joanne Rizzi, is "to show the manipulative aspect of commercials." In California, meanwhile, the state government is investigating Anheuser-Busch Cos. Inc.'s new giveaway program—called "Buy the Beer, Get the Gear"—in part out of concern over its appeal on college campuses. And in Washington, the Federal Trade Commission has proposed banning Joe Camel, while Bill Clinton has used the bully pulpit of the White House to chastise alcohol and tobacco companies for targeting kids.

Cover Story

None of those efforts, however, is likely to deflect the massive sales machine now directed at children. As long as kids have money to spend, marketers will fight to reach them. "Every 10 years, we begin to ask these questions, and no one has come up with a satisfactory answer," says Minnesota's John. The solution probably lies where it always has: with parents. They will simply have to be more vigilant than ever, knowing that wherever their children go—from day care to the Internet—there's now a marketer close behind.

By David Leonhardt in New York, with Kathleen Kerwin in Detroit and bureau reports

---

PSSST! COME INTO MY WEB...

With its unique ability to talk to computer-savvy kids one by one, the Internet should be a powerful marketing tool for anyone trying to reach the young and the hip. Instead, it has become the focus of critics who charge online kid marketers with abusive practices. Those issues were taken up in recent Federal Trade Commission hearings, but many marketers have already started overhauling their sites—in effect, undermining the one-to-one intimacy that makes the Net so compelling.

With some 4 million kids under age 17 going online last year alone, it's not surprising advertisers were right there with them. But exploiting the Web's interactivity without exploiting the immaturity of children has proven tough. Marketers have been slammed for offering freebies to kids in exchange for personal information without a parent's consent, and for not clearly differentiating ads from games or other entertainment.

One of the oldest kids' sites, from Web site developer Kidscom Co. in Milwaukee, asked registrants for personal information about themselves and their families from which it culled statistics for advertisers. Grey Advertising Inc. set up a kids' site purely for market research, soliciting info from children about their sneakers, cool words, and favorite music.

But in the wake of a scathing report last year by the Center for Media Education (CME), a Washington watchdog group, many mainstream marketers had to rethink how they interact with kids. Kidscom still asks questions, but before children can post messages or get free merchandise, they have to register—and Kidscom lets parents know by E-mail. Every time an ad appears, it's accompanied by a special character, the "ad bug." To search for pen pals, kids have to get their parents to send in a consent form. Grey, meanwhile, simply shut down its Web site.

A Presidential task force is expected to recommend guidelines for sites aimed at children next month, and the FTC is weighing rules for sites that market to children 11 and under. Earlier this month, CME and the Consumer Federation of America called for guidelines that would prohibit sending unsolicited commercial E-mail and offering free merchandise in exchange for personal information. In addition, the watchdog groups want marketers to obtain parental consent in writing or by E-mail before kids get access to sites where personal information is collected.

That may seem low-tech, but until the Web can overcome the perception that it's unsafe for kids, it's going to be unsafe for advertisers as well.

By Larry Armstrong in Los Angeles

WEB SITES FOR KIDS

www.dole5aday.com
Offers game with Bobby Banana and Barney Broccoli plus recipes.

www.mcdonalds.com
Includes a customized online newspaper

www.nabiscokids.com
Offers Oreo shooting game and Chips Ahoy screensaver

www.oscar-mayer.com
Kids can learn to surf with World Wide Weener Web tutorial

www.frito-lay.com
Kids can download wallpaper of site spokescharacter Chester

White House Effort Addresses Privacy

Gore to Announce Initiative Today

By ROBERT O'HARROW JR.
Washington Post Staff Writer

Vice President Gore will signal today a new Clinton administration effort to grapple with consumer privacy issues in the electronic age, announcing several measures to give individuals greater protection over how personal information is gathered and used.

Administration officials said Gore will use a commencement speech at New York University to announce a White House directive requiring every federal agency to name a person to assess whether existing privacy laws are being followed. He also plans to unveil a consumer clearinghouse of privacy tools and information on the World Wide Web (at *www.ftc.gov*), including one to help people to remove private information from public lists of drivers licenses.

And he will call on consumer, government and information industry officials to gather at a privacy conference in Washington next month to begin developing an "electronic bill of rights," which would seek to ensure privacy for the millions of people using the Internet.

Those initiatives represent the most prominent effort to date by the White House to address privacy, an issue that surveys show is a growing source of anxiety for millions of consumers. Administration officials said Gore, who also will call on Congress to quickly approve medical privacy legislation, believes that "privacy is an essential American value that needs be be updated for the information age."

Through improvements in technology, the number of companies gathering minute details about individual habits and spending patterns has skyrocketed. Most of that

Privacy advocates said the proposals fall short of what they believe is needed.

data is used by marketers, insurers and others. Information brokers on the Internet profit by reselling names, addresses and credit histories. The availability of personal information also has lead to a sharp increase in identity theft, a crime in which fraud artists assume an identity and run up bills in the names of unsuspecting victims.

Consumer and privacy advocates applauded details of the plan that emerged yesterday afternoon. They said the White House appears to be

See PRIVACY, *E4, Col. 1*

Privacy
— EW

Gore to Unveil Privacy Initiative

PRIVACY, *From E1*

giving long-overdue attention to the explosion of data collected about consumers—including magazine subscriptions, the groceries they buy, the amount of money they spend using credit cards and the Web sites they download from the Internet.

"The administration has opened its eyes to the importance of privacy at the end of the century and to the public's deep concern," said Janlori Goldman, director of the Health Privacy Project at Georgetown University. "It's more comprehensive than anything we've seen to date."

But Goldman and other privacy advocates said the proposals fall short of what they believe is needed. Several advocates said the White House should create a national privacy agency to oversee new policy. Others called for legislation that would restrict how database companies, credit bureaus and information brokers use personal data.

Marc Rotenberg, director of the Electronic Privacy Information Center, questioned the substance of the proposals, noting that federal agencies are already supposed to have on staff a person whose job is to address privacy matters.

"We need to look closely to see if these privacy options offer real protections," said Marc Rotenberg, director of the Electronic Privacy Information Center, a nonprofit advocacy group in Washington. "That's the key."

Gore's planned speech comes as the administration is struggling to justify its policy of allowing information companies to voluntarily restrict how they gather and resell personal information. A year ago, the administration said it would announce in July how the policy of self-regulation was working.

Officials have pledged that if the approach didn't create strong protections, they would consider new legislation.

But while Gore and other administration officials loathe the idea of imposing rules, fearing that regulation could restrict development of commerce on the Internet, privacy specialists and business officials alike agree that the results of self-regulation have been haphazard at best.

Tuesday, White House officials invited consumer and privacy advocates to a meeting to seek support for new efforts to promote privacy self-regulation by business. But advocates said they told officials they were skeptical that this approach could work.

"The administration invested their policy egos in self-regulation and they've got nothing to show for it," said Evan Hendricks, editor and publisher of Privacy Times, a Washington newsletter. "The tension is really building."

Advocates said consumers remain vulnerable to privacy intrusions everywhere they do business and so remain fearful about buying things on the Internet.

"One of the things that's missing is a coherence to it all," said Steven Cole, a senior vice president at the Council of Better Business Bureaus, which has begun working on a model for self-regulation that would impose sanctions on businesses that violate people's privacy expectations.

The speech also punctuates discussions about how the White House should respond to new privacy laws that take effect this fall in Europe.

The so-called European Directive would give consumers overseas greater access to personal information gathered by private entities. More important, the law could prohibit the export of data about citizens of European countries to any country that does not adequately protect privacy.

Because the law has never been tested, White House officials worry there's no way to know how that law would affect the information industry in the United States. If restrictions were imposed, it could be a major political embarrassment.

"It's crunch time," Hendricks said. "They're heading for a collision course with Europe."

Deirdre Mulligan, staff counsel at the Center for Democracy and Technology, was among those applauding the decision by the White House to focus more on privacy. But she said the administration has put itself in the position of catching up on very complex issues. "There needs to be a concerted, coordinated effort to get that house in order," she said.

FOR MORE INFORMATION
To read a Post special report on privacy in the digital age, click on the above symbol on the front page of The Post's Web site at http://www.washingtonpost.com

The distinguished author Peter Maas invites you to meet "Fred P. Smith." You don't know a thing about him, but if you wanted to, you could learn about his secret hoards, medical history, extramarital affairs, debts, all the places he has lived and much more. It's too easy.

How Private

"SECRETS" EASILY FOUND OUT

Despite the cherished right to privacy thought to be protected by the Fourth and Fifth Amendments to the U.S. Constitution, advanced computer technology today makes it possible to know just about anything about anybody, and in a fairly short time. Vast databases that most Americans don't even know exist can provide—to the scrupulous and unscrupulous alike—information on...

YOUR FINANCES. Including what you owe on all your credit cards, your payment record, other debts, even hidden bank accounts.

YOUR PAST. Is there a part of your earlier life that you would just as soon a prospective employer not know about? Forget it.

EXTRAMARITAL AFFAIRS. Accessible real-estate records can reveal a secret second apartment, and surveillance will do the rest.

MEDICAL RECORDS. Dates and addresses of medical visits are easily obtained. With HMOs, actual medical records are becoming easier to get.

I HAVE AN ACQUAINTANCE named Fred P. Smith. Actually, that's not his real name. I'm not using his real name because, as I have discovered in preparing this article, it is about the only shred of privacy he has left. And Fred Smith just as easily could be you or me.

The concept of the right to privacy was a treasured hallmark of the American way of life, institutionalized early on, indeed, by our Founding Fathers in the Fourth and Fifth Amendments to the U.S. Constitution. But that was long before the presence of hordes of private investigators and rapacious marketeers in an era of advanced computer technology that today draws on heretofore private information contained in vast databases that most Americans don't even know exist.

As a result, there are at this writing some 80 different patchwork bills pending in Congress aimed at restricting the flow of intimate personal data in cyberspace, now available to anyone browsing through the World Wide Web. Unfortunately, as the saying goes, the horse appears already to have departed the barn.

To learn precisely what was what, I visited the offices of Sutton Associates, located on New York's Long Island, which specializes in investigative services. Its president is James F. Murphy, a retired FBI agent. (As an agent, Murphy once had been a heroic headline figure. He had shot and killed one of two bank robbers holding a number of hostages at gunpoint as they tried to make their escape. The dramatic moment was later portrayed in the movie *Dog Day Afternoon*.)

As one of the most reputable firms of its sort in the nation, Sutton Associates limits itself primarily to background screenings for potential employment hirings and "due diligence" probes on behalf of corporate clients involved in buyouts, mergers, acquisitions and divestitures, all of which are considered quite legitimate. Sutton will not, on the other hand, accept divorce or criminal defense cases.

Recently, a company asked Sutton to locate a female consultant, now retired, who was urgently needed for a new project. The only information supplied was her name and that she was believed to reside somewhere in the vicinity of Washington, D.C. She wasn't listed in any phone books. It took no more than five minutes to come up with seven candidates with the same name, one of whom—the right one—met the appropriate retirement age of 64. But she had moved from her home in northern Virginia. So it took perhaps another five minutes to get a correct updated South Carolina address from one of the three major credit bureaus—Equifax, Experian and Trans Union—whose data banks record anyone who ever used a credit card.

My agreement with Jim Murphy was that Sutton Associates would demonstrate *how* a dossier could be compiled on an individual (not necessarily a job it actually would undertake). On occasion, a corporate client will ask Murphy if he can find out thus-and-such about someone. If Murphy considers the information beyond the bounds of propriety or legality, his standard reply is, "Yes, but I won't."

I supplied Murphy with the name of "Fred P. Smith." The only other information I provided was that he resided in the U.S. and was in the securities business. Sutton Associates had 72 hours to find out whatever it could about him.

The search began with what is called a "surname scan," which can be done nationally, regionally or locally based on data banks that have been compiled from such public source documents as voter registrations, motor-vehicle records (some states, like Maryland, actually sell these records) and real property listings.

Given the severe time constraints I had imposed and the fact that "Fred" was in the securities business, which could likely mean a Wall Street brokerage house, Sutton Associates elected to start with the greater New York City area. His middle initial helped narrow the field to 27 possibilities.

A so-called "credit header" search was then used to establish his occupation. These headers—essentially bare-

B Y P E T E R M A A S

COVER PHOTOGRAPH BY PAUL BARTON/THE STOCK MARKET; ALL PHOTOGRAPHS FROM THE STOCK MARKET ARE OF POSED MODELS

Is Your Life?

bones I.D. reports maintained by credit agencies—list not only occupations but also Social Security numbers, dates of birth and residential addresses. This information is also instantly available, for a modest fee, to subscribers to commercial databases, such as one called DBT-Online. An executive name search, using Dun & Bradstreet's *Dun's Market Identifiers*, confirmed that Smith was an officer in his brokerage firm.

A Cole's directory—actually a reverse directory in which phone numbers and addresses are cross-referenced for the whole country—is contained on sets of CD-ROMs. Once an address is known, the names of every other resident in that building or neighbors on a suburban block can be ascertained, opening the door to more intensive field investigations of any designated target.

A property search, such as those available from a Lexis-Nexis service, showed Fred Smith's previous residences, charting his rise from an apartment in a lower-middle-class neighborhood in one of the city's outer boroughs to a condominium on Manhattan's Upper East Side with a purchase price of more than $2 million. It also revealed that he owned a luxury sedan and a sport-utility vehicle, as well as another condo at a ski resort. Such information would come into play if he were subject to bankruptcy proceedings, tax liens or civil judgments. As it happened, his record was clear in these areas, nor was there any criminality.

It was revealed, however, that Fred—in his late 40s and married with two children—had a separate apartment in the city. Surveillance indicated that a young, attractive woman was in residence there. While adultery generally is not a financial factor in a divorce settlement, it could come into play if child custody became an issue. It might leave him open to blackmail as well.

Jim Murphy stopped Sutton Associates short of delving deeply into the lifestyle of Fred Smith. But if he had wanted to, Murphy could have learned about the restaurants Fred frequented, his airline travel, hotels he stayed at, his salary, ownership of stocks and bonds, his phone records, any evidence of addiction to drugs or alcohol (such as DWI arrests) or gambling, where his wife shopped and what she bought, how much money she spent, what schools their children attended, even the current state of their marriage.

But, in addition to circumspect firms like Sutton, there are other avenues open in the explosion of available personal information, chief among them "information wholesalers" that cater to private investigators, bill collectors, insurance agents and similar interested parties, such as business competitors.

One is Advanced Research Inc., located in Stroudsburg, Pa. It offers a range of intimate data that includes detailed credit-card activity, long-distance and intrastate toll calls, bank account numbers, deposits and balances, wire transfers, a beeper trace, a cellular phone trace, an employment history, business client lists, life insurance policies and a

STEPS TO PROTECT YOUR PRIVACY

1) Ask credit bureaus for a copy of your credit report, which lists companies that have asked for credit information about you. There may be a small fee. Call Equifax at 1-800-685-1111, Experian (formerly TRW) at 1-888-397-3742 or Trans Union at 1-800-888-4213.

2) Stop receiving unsolicited "preapproved" credit-card offers. Under a new law, all it takes is one phone call to have your name removed from credit-bureau mailing lists: For Equifax, 1-888-567-8688; Experian, 1-800-353-0809; Trans Union, 1-800-680-7293.

3) In filling out credit applications, look for a box that says this information is not to be disseminated.

4) Do not disclose personal information to retailers, such as your phone number and address. This information is often sold to both phone and direct-mail marketeers.

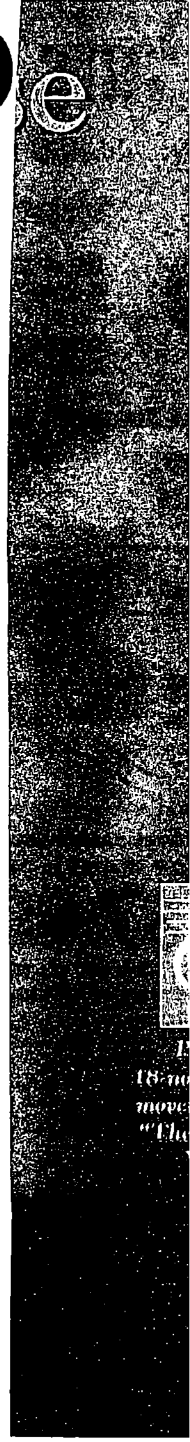
5) If possible, avoid litigation, such as a filed tax lien against you, which becomes public domain.

6) Avoid grocery purchases with a savings club card or credit card. Together with scanners, this tells marketeers your buying habits.

7) Request security codes (a number or a password) for your telephone and bank accounts. Potential intruders must repeat the password to gain access.

Barton/The Stock Market

Some 80 different bills are pending in Congress aimed at restricting the flow of intimate personal data in cyberspace. Unfortunately, the horse appears already to have left the barn.



Privacy
— CW

PHOTOCOPY PRESERVATION

medical treatment history going back as much as 10 years.

I decided to offer myself up as a guinea pig. I allotted Advanced Research 48 hours to come up with an unlisted phone number, a month's worth of toll calls and information about any bank accounts I had, either separate or held jointly with my wife. (I skipped a request for my medical treatment history when I learned that this would take four to six weeks. But I have no doubt that the firm would have delivered, based on its performance in other areas.)

As promised, it quickly came up with my unlisted number—not especially surprising, since I've had to include it on applications for various utility services and cable TV as well as warranties for purchases I had made (naïvely supposing it would not be disseminated elsewhere).

But two *other* unlisted numbers, which I have never given out, also were included. So were the toll calls I had made on all three lines, which, when matched with my phone bills, were right on the money. All my bank-account information—the account numbers, the banks involved, balances and deposits for the previous month—also was disturbingly accurate.

Michael Martin, who heads up Advanced Research, was coy about how this information was gathered. "These are well-guarded trade secrets," he told me. He said that he had specialists on call throughout the country who are allowed "to pursue their own methods." Defending his operation, he added: "In finding deadbeat dads, getting key evidence in child-custody cases, locating hidden assets in court-ordered judgments, why pay high attorney fees when we can do the job a lot quicker, a lot better and a lot cheaper?"

Jim Murphy of Sutton Associates said he was concerned about other (unnamed) companies, who engage in unscrupulous privacy incursions. "This is a business where you can't be partially pregnant,"

continued

he said. "If you have people who don't care, you're asking for regulations that will hurt all legitimate private investigators."

Murphy pointed to a Dallas businessman, John Spano, as an example of the importance of the kind of "due diligence" investigations Sutton Associates is engaged in. Spano, claiming assets of more than $250 million in Treasury bills and offshore accounts, received loans of $8 million from a Dallas bank and $80 million from a Boston bank toward acquiring a National Hockey League franchise, the New York Islanders. It all fell apart when Spano failed to meet a $16.8 million installment payment for the team on a total purchase price of $165 million and pleaded guilty to fraud. It was then reported in court that his assets totaled barely more than $1 million. The NHL had conducted only a cursory investigation of Spano's assets before approving his purchase of the team.

Still, as alarm over privacy invasion grows, 14 of the largest database companies, fearful of restrictive legislation, recently have agreed to attempt to regulate themselves by adopting guidelines that would limit access to personal information by the general public.

The rub is that private investigators are an exception to the rule. According to *P.I. Magazine*, there are about 60,000 licensed private eyes operating in the U.S. The qualifications vary from state to state. Some states—like Colorado, Alabama, Mississippi, Idaho and South Dakota—don't require licenses at all.

There remain certain steps an individual can take to protect against unwarranted privacy invasions (see box on page 5). The great irony is that a fundamental building block in creating a personal dossier is your Social Security number. Yet when the Social Security Act of 1935 originally was passed by Congress, an individual's number was not to be used as an identifier for other than Social Security purposes.

Who could have imagined what would subsequently happen? Today, to apply for just about anything, you are required to give the number up.

Contributing Editor Peter Maas' best-selling books include "The Valachi Papers," "Serpico," "Killer Spy" and, most recently, "Underboss," now in paperback.

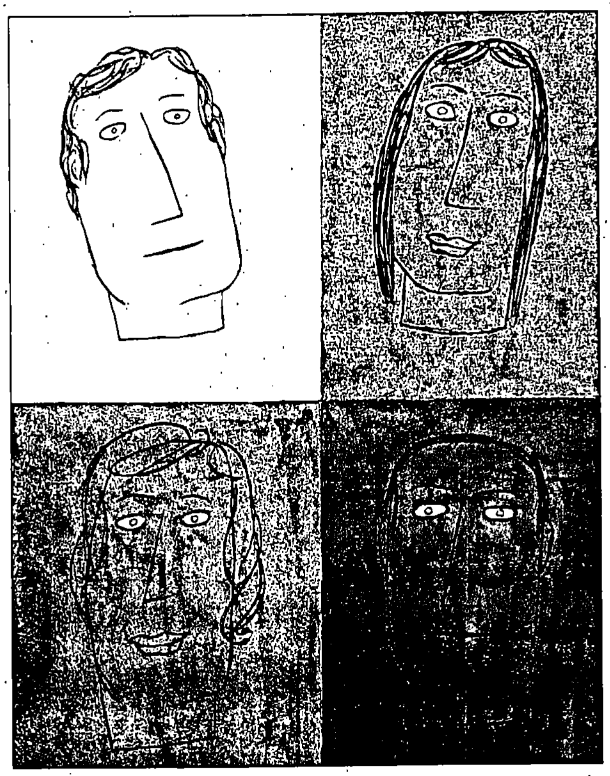
THE MILLENNIUM NOTEBOOK

Stick 'Em Up? Not Anymore. Now It's Crime by Keyboard.

KATHRYN RAMBO GOT A taste of the future recently, and she didn't like it one bit. Sure, she had a new $22,000 Jeep, five credit cards, an apartment and a $3,000 loan listed in her name. Problem was, the 28-year-old special-events planner from Los Gatos, Calif., hadn't asked for any of it. A woman impersonating her had, with the help of information lifted from Rambo's employee-benefits form. Straightening out the mess took months of angry phone calls, court appearances and legal expenses. And then there was the Kafkaesque chore of proving that she was, in fact, herself. Says Rambo: "I was going around saying, 'I am who I am!' "

Rambo was a victim of "identity theft," an increasingly common crime committed by increasingly sophisticated swindlers. All they need is your full name or Social Security number, which they drop into Internet databases that serve up info like your address, phone number, employer or driver's license number. Then they're on their way—applying for credit using your good name. Security experts say identity theft's high profitability and low penalties could make it as common as auto theft in the coming century. "It'll be the next growth industry in crime," says Ann Cavoukian, privacy commissioner of Ontario and coauthor of "Who Knows: Safeguarding Your Privacy in a Networked World."

And identity theft is only one new form of millennial malfeasance. While new technology and widening global trade have made enterprise more efficient, both have also opened new cracks in society's defenses. Take commerce. As much as $117 billion in financial transactions will occur online by the year 2000, according to market researchers IDC. As banks go digital—in operations like trading stocks, paying bills, making loans—the robbers will, too. "If Willie Sutton were alive today, he'd be learning HTML coding," says Paul Saffo, a technology forecaster in Menlo Park, Calif. The sheer size and speed of information networks will make them impossible to monitor closely. Indeed, all sorts of transgressions are already occurring in the shadowy corners of the Internet. Cyber-pirates, for example, register phantom ships on the computers of maritime agencies. After taking out huge insurance policies on these virtual boats, the crooks "sink" them with the stroke of a computer key and file multimillion-dollar claims. Poachers in Zambia now take e-mail orders, à la L.L. Bean. A bigger threat may be electronic money laundering. As the Internet becomes a place where money changes hands, strong cryptography will become the digital equivalent of armored cars: a way for people to protect their transactions. Which is exactly what worries the Feds. They don't want encryption to be too strong, lest money launderers use it to transfer funds under their radar. To an extent, this is already happening. "We're simply losing the ability to break into their information structures," says John Arquilla, a Rand Corp. consultant.



Four characters in search of their stolen identities

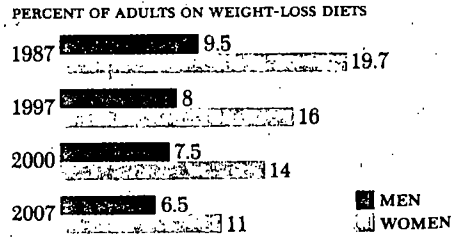
Our increasing reliance on computers may also leave us vulnerable to the terrorists of the future. Computer viruses, though so far not the problem once projected, are one threat. Another is the electromagnetic pulse weapon, which would use ultra-high-frequency radio waves to scramble hard drives and fry computer chips. It wouldn't kill anyone directly, but it could jeopardize lives by knocking out vital movements of natural gas, oil and electricity.

But don't panic yet. Identity theft, for instance, won't catch on right away; crooks are by and large a conservative bunch, attached to their Saturday-night specials. And by the time it does, authorities may have installed something called biometric identification. Straight out of "Mission: Impossible," biometric ID turns body parts into PIN numbers. Retina and palm scans already grant entrance to buildings. Even body odor or DNA samples could become "passwords." "Effectively," says George J. Tomko of Mytec Technologies, "people would walk around without any paper ID at all." In that world, at least, Kathryn Rambo would be safe—as long as no one stole her eyeballs.

T. TRENT GEGAX

Dissing Diets

Though increasing numbers of Americans are obese, fewer are trimming down by watching what they eat.



SOURCE: MEDIAMARK RESEARCH, AMERICAN DEMOGRAPHICS

ILLUSTRATION BY BENOIT

Equifax Inc., Trans Union and TRW Inc. — to find strangers with good credit histories, living as far away as Alaska and Washington. They [illegible] credit accounts in the customers' names, ordered thousands of dollars in products and left the victims to struggle to restore their credit ratings. What made the 1993 case unusual was that the culprits were caught. Quick credit and ready access to Social Security numbers have made "theft of identity" one of the fastest growing forms of credit fraud, according to the U.S. Public Interest Research Group, a consumer advocacy organization. Officials at Trans Union said the credit bureau gets 45,000 to 50,000 calls a month from people complaining that their accounts have been taken over.

¶A convicted child rapist working at a Boston area hospital in 1995 was accused of using a former employee's computer password to rifle through nearly 1,000 confidential files of patients for telephone numbers he used to make obscene calls to girls as young as 8 years old. Like many hospital systems, this one neither locked out defunct passwords nor triggered a warning when one person called up an unusual number of files. In an even more startling case, reported by The New York Times last year, a convicted pedophile in a Minnesota prison was accused of compiling a computerized data base of more than 5,000 children and babies, annotated with descriptions like "cute," "latchkey kids" and "Little Miss pageant winner." The lists, apparently pieced together from items in small-town newspapers, were stored with child pornography obtained over the Internet.

¶Earlier this year, the Sara Lee Corporation asked a health maintenance company to survey and screen all 500 employees in its Mesilla Park, N.M., hosiery factory, for signs of depression that might underlie sick days and affect job performance. The plan was for the employees' personal physicians to consider prescribing antidepressants, according to an account in Fortune magazine that stressed the potential medical cost savings of the pilot project by Lovelace Health Systems, a subsidiary of the Cigna Corporation. Later, Anne Mu[illegible], a spokeswoman for Lovelace, said the magazine account caused the project to be put on hold: the employees at the nonunion factory were not supposed to know the true purpose of the survey. "They didn't want it to be seen as a depression screening," she said, "they wanted it to be seen as a health-risk screening."

According to successive polls conducted by Louis Harris for Equifax in 1994 and 1995, 4 out of 5 Americans are concerned about threats to their personal privacy. This is a growing public relations problem for business, which has its own brand of privacy concerns: the ability to keep proprietary information "private" in a networked world competing for a data edge.

But a strong undercurrent dismisses privacy as "the ultimate subjective, touchy-feely issue," as Robert J. Posch, Jr., a vice president at Doubleday and marketing law specialist, put it. In the trade magazine Direct Marketing, he scoffed that privacy was "just some notion of the right to be left alone. Spare me."

Both legal scholars and computer scientists who advocate more privacy rights for individuals contend that in the information economy, privacy is less about seclusion than about power, and the personal autonomy necessary to democracy.

"Through the use of data banks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children," wrote Paul M. Schwartz and Joel R. Reidenberg, two American lawyers who were commissioned by the European Union to study American data privacy law and who published their critical findings in a book last year. "Companies take the position that the use of personal information is in the best interests of customers. Yet these companies deny consumers the opportunity to judge for themselves."

The Clinton Administration has called for a balance between individual privacy and the needs of an increasingly information-driven economy, but like the two previous administrations, it has made industry self-regulation the centerpiece of its privacy policy.

Critics contend that self-regulation amounts to little more than public relations, and that the titans of information are despoiling democracy's inner landscape with as little restraint as the coal barons and oil trusts showed during laissez-faire industrial growth.

Ms. Dennis's case offers a rare look at the human dimension of the conflict, and provides a road map to the hidden places along the way where gold is spun from the raw data of people's lives.

A Prison

In a Growth Industry, Inmates Process Data

In the heat-soaked shimmer of an August noon in 1996, in a field outside a Texas penitentiary, prisoners with hoes stood double file, before a lone guard on horseback. It was a tableau from an earlier era.

Okra and cotton are still raised by some of the 136,000 inmates serving time in the fifty-two prisons within the Texas Department of Criminal Justice. License plates still clatter from noisy machines manned by convicts inside the big Huntsville prison, southeast of Dallas, where visitors are given a bumper sticker that reads "Texas — It's Like Another Country." But since 1968, when a Records Conversion Facility opened at the Wynne prison unit in Huntsville, information has been part of Texas prison industries.

On this day, thousands of boxes of public records were passing through the vast, low-slung steel-frame building, one of five such prison operations in the state, and one of dozens across the country. Under hanging fluorescent lights, an acre of men in dingy prison whites turned documents from public agencies into microfilm images and computer bytes.

"Anything and everything could be in here," said DeeWayne Beckham, the assistant plant manager. At random, he picked up a record from the Bexar County courts in San Antonio. It was a petition in a 1991 divorce case asking for child support for a girl named Megan.

There were patient progress reports from the Brenham State School for the mentally disabled in Brenham, Tex., motor vehicle titles from the Texas Department of Transportation, criminal investigation records from police and the state attorney general's office. The last were stacked high behind a special wire mesh cage, for fear, Mr. Beckham said, that inmates would steal crime scene photographs and sell them.

"I've got murderers, and whatever else you can imagine," Mr. Beckham said cheerfully, passing a man with tattoos on three fingers in a group unstapling and sorting documents at a long table. Other prisoners fed the pages into microfilm machines that capture as many as 17,000 pages a day.

Nearby, inmates typed at computer keyboards, producing computer tapes from 30,000 applications for the government's Women, Infants and Children nutrition program for low-income pregnant women and young children.

This was the data-entry section where, under the unit's first and only private sector contract, inmates in three shifts handled thousands of the Metromail "Shoppermail" questionnaires each day in 1993 and 1994, as well as other Metromail surveys commissioned by Seventeen magazine, L'Oreal, Six Flags, Days Inns, R.J. Reynolds and Time-Life. The prison was paid $150,000 for the work.

Hal Parfait, the inmate serving seven years for breaking into a woman's house and raping her after threatening to kill her children, was transferred elsewhere after he wrote letters to at least two women whose identities and habits he had learned from the surveys.

But for about three months after his letter to Beverly Dennis came to light in 1994, the work continued pretty much the same way, records show. Then the Texas Legislature, responding to news accounts, barred sex offenders from record-entry work in prison. Overnight, Mr. Beckham lost 167 of his 430 inmate employees, and eventually 187 of them.

It was the same in the other Texas prisons, said John Benestante, director of state prison industries. "We lost some damn good programmers — pedophiles," he said. "Some of our best computer operatives were sex offenders."

But now Ms. Dennis was suing the Texas prison, and Mr. Benestante, a 6-foot-3 former air traffic controller, was deep in a review of all prison industry operations, especially those handling information for other public agencies, which pay by shifting public funds to the Department of Corrections.

Problems in the past had ranged from obscene "nasty-grams," inserted at random by prisoners stuffing envelopes for the Texas tourism department, to a ring accused of supplying car thieves with motor vehicle titles on commission. Well before the Dennis case, an inmate had used information on a motor vehicle title to contact a woman, and in a different department, an inmate managed to memorize a supervisor's Social Security number from a time sheet and ruin his credit rating.

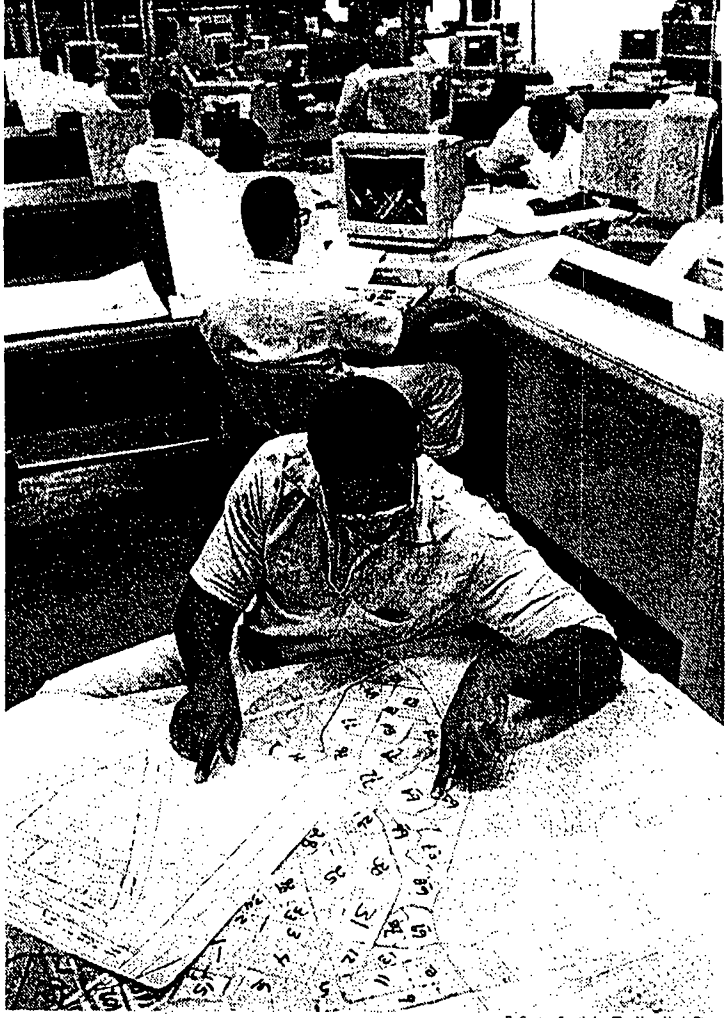
Aside from the risks, he said, there were signs of shrinking demand, as more public agencies kept their records computerized from the start. But private companies were still eager to extract and compile valuable information from public records.

So Mr. Benestante had found a new high-tech information field with a promising commercial market, and had put the Ferguson prison, near Midway, Tex., ahead of the curve. Its former boot factory was a site for work in Geographic Information Systems, or G.I.S., a cutting-edge technology putting detailed maps and high resolution aerial photographs into computerized form.

How detailed? Plat records for Dallas show the location of the gas meter on each parcel. Aerial photographs of the city of Bryan, Texas, show the exact footprint of each house.

After the computer maps leave the prison, explained Robert Laake, the assistant administrator of the Ferguson "automated mapping-G.I.S." operation, "the Dallas planning and development department will place unique identifiers in each lot that will give them all the information they need — who lives there, what that block is worth."

The Ferguson prison has floor-to-ceiling



F. Carter Smith for The New York Times

At the Ferguson state prison near Midway, Tex., inmates use a cutting-edge technology to put detailed maps and aerial photographs into computerized form.

F. Carter Smith for The New York Times

At the Texas prison in Huntsville thousands of boxes of public records were processed before the business moved to another prison.

crash gates and tiers of two-man, 5-by-9-foot cells. The work site can be reached only by passing through a shower area lined with urinals, and walking across a yard where the men are routinely strip-searched on their way to and from the job. On the day of the visit, no inmates were at work because of a "lock-down" imposed after a rash of stabbings.

But inside the building, one could have been in any office. Supervisors demonstrated the simple computer tasks performed by the inmates, 120 men with an average sentence of 32 years. The price of their work was right. The unit was digitizing Van Zandt County's maps for $19,880, compared to a private sector bid of $60,000.

"If you don't send this here, the next stop is India," said Marilyn Beckham, the plant manager, referring to "information sweatshops" in Asia, Mexico and the Caribbean where much data entry is now done.

The strong privacy concerns raised about G.I.S. have little to do with using prisoners for the grunt work. This technology is proving an astonishingly powerful and lucrative commercial tool to crunch information from public records and private sector data banks and to spit out house-by-house information that can include everything from the tax assessment and the occupant's driver's license photograph, to details of consumer behavior collected by the likes of Metromail.

But Angela Pugh, a supervisor for the G.I.S. project at Ferguson, shrugged off the issue.

"Is the government going to sacrifice the money that can be made for a little bit of privacy?" Ms. Pugh asked.

A Business Technology

Using Compiled Data To Map Out Profiles

On an idyllic campus in Orono, Me., a professor who helped nurture the technology known as G.I.S. now wrestles with its dangers.

As Harlan Onsrud tells it, G.I.S. is a case study on the way new technology can change old stores of information into commercial gold and social dynamite. The story of its success, he said, underscores that both technological advances and sweeping business mergers have exploded old boundaries, leaving in the dust the sector-by-sector privacy legislation of the last three decades.

G.I.S. started as a way to map land, sea and sky across space and time. It has had enormously beneficial social uses, from pinpointing the origin of Legionnaire's disease to helping South Florida communities coordinate emergency relief after Hurricane Andrew.

But "there is no doubt that some uses, although currently legal, would be considered by most citizens in the U.S. to be highly intrusive and inappropriate," contended Mr. Onsrud, chairman of the University of Maine's department of Spatial Information Science and Engineering, part of the National Center for Geographic Information and Analysis.

In one G.I.S. application, businesses can feed car license numbers from a parking lot into a program and retrieve a customer's name, address, census tract information and demographic characterizations like "Hardscrabble," "Sharecroppers," and "Furs and Station Wagons." Another program transforms a telephone number into a detailed profile of each prospective customer who calls an 800 number.

Public spaces are increasingly monitored electronically — for convenience, safety and traffic planning. But G.I.S. allows the results of this surveillance to be mapped with precision, identified by an individual's name or vehicle number without their knowledge, and correlated to a wealth of other information, including data culled from computerized public records of the kind the Texas prisoners have processed for 30 years.

Increasingly, cash-strapped government agencies are selling packaged public information to businesses or entering joint ventures to make the information more attractive to marketers.

Only a decade ago, when the Federal Bureau of Investigation sought clearance to enter all national databases, Congress said no.

"Now the commercial market has done it for them," Mr. Onsrud said. Government agencies like the F.B.I. "just have to pay like anybody else."

In the last three years or so, G.I.S. has spawned a booming "Geo Business" industry that applies its power to profile people and households for data-based marketing, health care, insurance, real estate and financial services. All three major credit bureaus and other giants in the information field have acquired or merged with G.I.S. mapping companies. They have forged new partnerships with big suppliers of data and data-mining software, and bought companies that deliver information to desktop computers on CD's or over the Internet. Their products include data bases that are continuously updated and parsed to yield an unprecedented level of detail on nearly everyone in the nation.

If information is like money, a company called the Acxiom Corporation is one of the merchant bankers of the age. Set in an industrial park in Conway, Ark., north of Little Rock, the corporate headquarters has a cathedral lobby with a facade of glass. But its heart is behind the locked doors of what a guide calls "the production war rooms," low-ceilinged bunkers where six robots inside small linked silos match data tapes at 60 miles an hour, while 20 mainframe computers swallow 1.3 billion bytes of data a second. G.I.S. is just part of the information infrastructure.

Acxiom's revenue grew by almost 50 percent in fiscal 1997, to $402 million. Its top customers include data kings like the AT&T Corporation, Wal-Mart Stores, Citibank, a unit of Citicorp, I.B.M., the Allstate Corporation and Automatic Data Processing Inc., which handles half the payrolls in America. The company now crunches all data for Trans Union. And last year R. R. Polk and Company, which says it collects and markets automotive and consumer information on 95 percent of the nation's households, used eight tractor-trailers to move its mother lode of data tapes from Michigan to a special warehouse in Conway.

This is a place where visitors are issued badges that turn purple if they leave the building — part of the aura of security Acxiom wants to convey to customers nervous about leaving their treasured customer data bases where their competitors also come to buy and barter for more data on their own customers, more names to "populate" computer models of their best prospects.

Many members of the information industry say technology is simply recreating the intimacy of small-town America in the days when the storekeeper knew all his customers by name, habit and history. But Mr. Onsrud, whose village in coastal Maine actually embodies that small-town ideal, flatly rejects the analogy.

"It's not an equal or mutual relationship," he said. "We have information insiders and outsiders."

A Life and a Lawsuit

A Woman's Privacy Invaded By Industry

Beverly Dennis grew up in almost preindustrial scarcity in a house her grandfather built himself. It had no electricity, no running water, and no indoor toilet to the day he died at 99. He never owned a car.

"I was raised very poor," Ms. Dennis said, sitting at the dining table in her carefully tended home. "My grandma used to boil her clothes on a stove, scrub on a washboard in the cold of winter. We didn't have much, but there was so much love."

Now Ms. Dennis has all the creature comforts of the industrial revolution, but she works standing at a noisy machine, stamping out 1,500 plastic bobbins an hour for less than $80 a day. "It's fast-paced work," said Ms. Dennis whose finger was recently mangled on the job. "I don't know how long I'll be able to do it."

For a few months several years ago, she had happily joined the brave new information economy at the Canton, Ohio, office of a national collection agency, G.E. Capital, owned by the General Electric Company. Computers automatically dialed telephone numbers from a disk, and each debtor's name, address, and payment history ap-
·d on her computer screen. Ms. Dennis

Tony Dejak for The New York Times

Beverly Dennis, of Massillon, Ohio, filed a class-action suit against Metromail, a data-marketing company, after an inmate processing its information used it to harass her.

Karen van Donge/The Arkansas Democrat-Gazette

Byron Mabry works for Acxiom, an information-processing company based in Conway, Ark., whose clients include AT&T, Allstate, I.B.M. and Wal-Mart Stores.

was monitored electronically as she followed a script demanding payment for everything from Apple Macintosh computers to children's shoes.

She failed to pass probation. "They told me I was too nice to be a collector," said Ms. Dennis, who raised two daughters on her own.

But this soft-spoken woman has a stubborn sense of justice, and it has carried her through tough times in a lawsuit that is trying to break new ground.

Last August, two of Metromail's lawyers questioned her for almost seven hours during a deposition in Austin, Tex. They wanted to know her Social Security number, her unlisted telephone number, when she had last dated and whether she drank. They probed into her health care and medication history, and had her name all her fellow employees. One of the Catch-22's of privacy litigation is its sacrifice of privacy.

Ms. Dennis, who earns less than $16,000 a year, said after she learned the identity of the inmate, she borrowed money to put in security lights, deadbolt locks, new windows and an alarm system in an unsuccessful effort to allay her pervasive sense of fear. Mr. Parfait, originally due to be released in 1995, is now to be freed next year.

"It's made me a different person," she said, describing sleepless nights, more frequent migraines and lost wages. "I can only tell you that I would give everything that I have if this would never have happened to me, because I am scared each and every day of everything, and I trust nobody after this."

Ms. Dennis said she wanted to warn other people so they would not make her mistake.

But Shannon H. Ratliff, a lawyer for Metromail, suggested she had shown indifference to her privacy by giving her unlisted telephone number to Mark DeMarino, an investigative reporter at the Cleveland television station WJW-TV who helped her uncover the Metromail link, and by appearing with him on Geraldo Rivera's television show. The lawyer even asked why she had not sued the local station, since information from its reporter had upset her.

This was a line of attack rooted in the weaknesses of privacy case law, which has tended to see privacy as a "right to be left alone," in Justice Louis D. Brandeis's famous phrase — and to let that right collapse the moment personal information is surrendered for any reason.

But the critical issue today, privacy law experts agree, is usually not whether personal data should be collected and processed, but how data should and should not be used. Preserving privacy in this context is about the autonomy necessary to make decisions. That, too, has been recognized as a privacy interest by the Supreme Court — most notably in its decisions on abortion and contraception — but has not been developed much beyond decisions involving family and sex.

Privacy laws have been so narrow and spotty that the names of the movies rented at the video store where Ms. Dennis works on weekends are legally protected, but pay-per-view movies ordered at home are not. Medical and pharmacy records are not protected either and though the privacy of credit reports has been a matter of Federal law since 1970, a huge market in the information they contain has grown through its loopholes.

"The law of privacy has not kept up with the modern advances in technology, the modern rise of data transfer and information collection," Michael Lenett, Ms. Dennis's lawyer at the Cuneo Law Group in Washington, argued when the suit was filed last year. "This is the first case squarely to present the issue, who owns your personal and private information? Who controls it?"

But in April, when Mr. Lenett was still battling to get internal company documents, a judge in Travis County threw out the case's claim against the prison; an appeal is planned. The court ruled in part that misuse of information did not constitute misuse of property under the Texas Tort Claims Act, which makes the state immune from most damage suits.

"She's not complaining that somebody took a data-entry machine and whacked her on the head with it," explained Lin Hughes of Austin, Tex., a lawyer for Metromail.

The ruling leaves the claims against Metromail and its former parent, R. R Donnelley & Sons: that the company unjustly enriched itself, and violated the privacy interests of the members of the class by fraudulently inducing them to provide personal information without disclosing how it would be processed and sold, and that it recklessly endangered their safety and inflicted emotional distress by negligently allowing felons to handle the information. The lawsuit seeks damages to be determined later and injunctive relief, including notification to all whose surveys went through the prison.

The company insisted in an unsuccessful motion to dismiss the case that it had no legal duty to tell consumers that the surveys would be processed by inmates. The facts consumers disclosed were not "highly intimate or embarrassing," the company argued, nor were they disclosed to the public at large.

Another cause of action recognized in Texas is conduct so "extreme and outrageous" that it is intolerable, and inflicts severe emotional distress. But, the company argued, "The mere receipt of a letter in the mail from an incarcerated inmate is not so extreme as to satisfy this standard."

Outside the courtroom, the company said its subcontractor was responsible for the prison work, and said that the job was stopped the same day Metromail learned of it. Internal documents tell a different story: Data tapes and surveys at the Texas prison were among the assets Metromail bought in 1993 when it acquired CMT, a marketing list company, and shipments and letters between the prison plant and Metromail continued until the work was finished, about three months after the letter came to light.

Documents gained through discovery also brought the four additional named plaintiffs to the case.

"I know the potential is out there to abuse people's information, but I really never gave it too much thought until I realized that my own information passed through the hands of a rapist or murderer," said one plaintiff, Patricia Mendiola, a part-time hospital lab technician in Wheaton, Ill., who is married to a systems analyst and has two children. "It made me so mad, the realization that all of this information ends up in a big data bank."

Robert DeSantis, who lives in Silicon Valley and was a civilian employee of two California military bases that closed, said that as a gay man, he worried about hate groups that could use such data bases to harass minorities.

Frenchie Holmes, a former fraud investigator for Pacific Bell in San Jose, Calif., who is now on disability, said she had been gullible. "You think they're going to send you products and trash that information, but they sell it. You fill out just one questionnaire and all of a sudden the whole world knows who you are."

Tim Fitzpatrick, a Metromail spokesman, said such sentiments were not common. "We certainly do not feel there's a class of people harmed as a result of this," he said. "Millions of people every year utilize direct marketing as a way to get things done. Millions of people are benefiting from it."

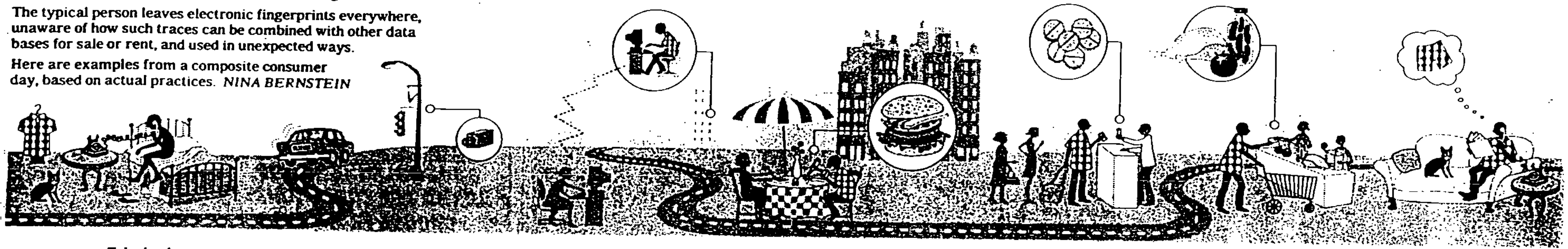
Indeed, Ms. Dennis counts herself as one of them. With two jobs, she shops by mail. "A new pair of curtains can make me so happy," she said. She does not know why the price should include her privacy.

"They are making millions of dollars off other people's lives who don't even know what they're doing," Ms. Dennis said. "They have t[illegible] my whole life upside down."

A Day in the Life of Joe Consumer

The typical person leaves electronic fingerprints everywhere, unaware of how such traces can be combined with other data bases for sale or rent, and used in unexpected ways.

Here are examples from a composite consumer day, based on actual practices. *NINA BERNSTEIN*



	Telephoning	Driving	Sending E-mail	Dining	Getting Prescriptions	Shopping	Mail Ordering
ACTIVITY	Joe calls an 800 number to check the pollen count.	Rushing to work, Joe inadvertently runs a red light.	At work, Joe criticizes his boss in E-mail to a friend.	Joe eats lunch at a restaurant that records each order on a computer.	Joe stops at the pharmacy to fill a tranquilizer prescription	At the supermarket, Joe uses a discount shopper's card.	Before bed, Joe orders cufflinks and silk boxer shorts from a catalogue.
DATA CAPTURE	Joe's number is caught through Caller ID; his name and address are pulled from a public records data base.	Though the intersection is empty, a video camera captures his license number.	Joe's company reviews employee Internet activity and keeps copies of all E-mail.	Joe pays by credit card, linking his account number to his order of a bacon cheeseburger and fries.	His name, the drug and his doctor become part of the data base of the pharmacy chain	The card links Joe's identity to every item he buys.	He pays by American Express, which adds his name to lists of "buyers of expensive jewelry."
FIRST USE	Joe is put on a list of allergy sufferers; it is sold to a drug company marketing allergy pills.	Joe is sent a traffic ticket in the mail.	After Joe's boss reads the E-mail, Joe is dismissed.	The restaurant checks his credit standing and sends him a discount offer.	The chain is part of a pharmaceutical company that combines the data with lists of magazine subscribers.	The supermarket chain uses a data-mining service to create profiles of its most profitable customers.	The catalogue company puts his name on a list of "male buyers of sexy lingerie" and trades it with other companies.
LATER USE	The list is linked with a profile of Joe and he is sent a coupon for the company's allergy medication.	Joe's insurance company finds the violation in a data base search and raises his rates.	Joe's unsuccessful lawsuit to regain his job shows up when a prospective employer uses an Internet investigation service.	The restaurant goes bankrupt and its list of men who are bacon cheeseburger lovers goes on the information market.	A rival tranquilizer company advertises in Joe's favorite magazine; company mailings urge Joe's doctor to switch.	Joe is deemed a prized customer and gets electronically-generated discounts, less loyal customers pay more.	Within two weeks Joe will receive four jewelry catalogues, five lingerie catalogues and a sex-videotape offer

The New York Times; Illustration by Megan Jaegerman

The New York Times

THURSDAY, JUNE 12, 1997

Personal Files Via Computer Offer Money and Pose Threat

By NINA BERNSTEIN

LIVES ON FILE

The Erosion of Privacy

A special report.

It was past midnight when Beverly Dennis came home, weary from her second-shift factory job, and found a letter with a Texas postmark among the bills and circulars in the day's mail. As she read it in her small house in Massillon, Ohio, alone in the dark stare of the sliding glass doors, her curiosity turned to fear.

The letter was from a stranger who seemed to know all about her, from her birthday to the names of her favorite magazines, from the fact that she was divorced to the kind of soap she used in the shower. And he had woven these details of her private life into 12 handwritten pages of intimately threatening sexual fantasy.

"It can only be in letters at the moment," the man wrote after describing the sexual acts he planned. "Maybe later, I can get over to see you."

The explanation that eventually emerged deepened Ms. Dennis's sense of violation — and places her experience at the heart of a far-reaching national debate over legal protection for privacy in a world where personal information is ever easier to mine and market.

The letter writer was a convicted rapist and burglar serving time in a Texas state prison. He had learned Ms. Dennis's name, address and other personal information from one of the product questionnaires that she and millions of other consumers had received in the mail, innocently completed and sent back to post office boxes in Nebraska and New York on the promise of coupons and free samples. Their answers were delivered by the truckload to the Texas prison system, which was under contract to handle the surveys for the Metromail Corporation, a leading seller of direct marketing information. Hundreds of unpaid inmates, many of them sex offenders, entered the information on computer tapes for Metromail, which has a detailed data base on more than 90 percent of American households.

To Ms. Dennis, a woman in her 50's who grew up in the coal country of southern Ohio, it was as though her privacy had been strip mined by the dark side of the information economy.

Indeed, as the free-flowing exchange and exploitation of information is being celebrated as the main engine of economic prosperity into the next century, individual privacy is looking more and more like an endangered natural resource.

Hunger for personal information is now growing explosively in almost every sector of the nation's economy and everyday life, from health care to entertainment, from banking to supermarket sales. It is being

Continued on Page A30

21. Does anyone in your household have:

	You	Adult 2	Other	Prescription Drug Used
Allergies	01	21	41	61
Angina	02	22	42	62
Arthritis	03	23	43	63
Asthma	04	24	44	64
Back Pains	05	25	45	65
Birth Defects	06	26	46	66
Bladder Control Prob.	07	27	47	67
Clinical Depression	08	28	48	68
Diabetes	09	29	49	69
Epilepsy	10	30	50	70
Frequent Heartburn	11	31	51	71
High Blood Pressure	12	32	52	72
High Cholesterol	13	33	53	73
Migraines	14	34	54	74
Osteoporosis	15	35	55	75
Prostate Problems	16	36	56	76
Psoriasis	17	37	57	77
Ulcers	18	38	58	78
Yeast Infections	19	39	59	79

22. Does anyone in your household take any of the following prescription medications?

	You	Adult 2	Other
Claritin	01	11	21
Estrogen Replacement	02	12	22
Glucotrol	03	13	23
Hismanal	04	14	24
Insulin	05	15	25
Paxil	06	16	26
Prozac	07	17	27
Seldane	08	18	28
Tagamet	09	19	29
Zantac	10	20	30

A Texas woman's answers to this 77-question consumer survey ended up in the hands of felons.

spurred and sharpened by powerful market forces and ever more pervasive computer technology, including digital mapping tools and so-called "data-mining" software that blast commercial value from newly linked data bases of unprecedented size.

Yet like the people whose private lives and public records passed through the fingers of Texas felons, most Americans have no idea what is happening to the stream of personal data that they shed just by living in the modern world. And most businesses that make money on the collection, recombination and sale of shards of personal information maintain that people need no legal right to know, and have no good reason to object.

The electronic deposits keep growing with the pulse of daily life: telephone calls, checkout counters, A.T.M.'s, and electronic bridge tolls, the street gaze of security cameras, plastic insurance cards imprinted with the Social Security numbers that have become identity's common currency — and its easy counterfeit.

The Internet, where every keystroke can be archived, is now the most dramatic embodiment of what technology and commerce afford in the real world: the pooling of ever more vast stores of data, and the easy retrieval of individual specks with no one's say-so.

This networked world of information is an economic powerhouse that creates new jobs, new services and astonishing efficiencies. It offers a wide range of consumer benefits, including easy credit, shopping convenience and customized goods and services. It also turns commonplace transactions into little revelations.

When a clerk puts a supermarket discount card through the scanner, for example, a data base links the shopper's identity with the bar code on every item bought. A love of rich chocolate cookies not only can be tracked over time, but matched with an individual's address, age, weight and ethnicity, with marital status and credit standing and even with religious ties, to name just a few of the personal facts being bought and sold wholesale in today's booming information market.

A class-action lawsuit that Ms. Dennis filed last year against Metromail and its subcontractors is emblematic of the growing conflict over privacy as people learn how little they control the use of personal information that is an increasingly valuable corporate asset.

"Privacy will be to the information economy what consumer protection and product safety were to the industrial age," Marc Rotenberg, director of the Electronic Privacy Information Center in Washington, warned at Federal Trade Commission hearings on electronic consumer privacy last year. This week, the F.T.C. is holding another round of hearings on the issue.

But as Ms Dennis has learned during a three-year struggle for redress, any battle for privacy today is an uphill fight, and individuals have an inherent disadvantage.

Ms. Dennis spent sleepless nights trying to figure out the stranger's identity. She finally turned to local television news reporters for investigative help, and searched for more than a year before she found a lawyer willing to take on a novel and demanding case without pay.

But when Metromail executives wanted to know more about the woman suing the company, their task was simple: They turned to the company's own massive consumer data base, and retrieved more than 900 tidbits of Ms. Dennis's life going back to 1987. Laid out on 25 closely printed pages of spreadsheets were not only her income, marital status, hobbies and ailments, but whether she had dentures, the brands of antacid tablets she had taken, how often she had used room deodorizers, sleeping aids and hemorrhoid remedies.

"Attached is all we know concerning Beverly Dennis," Dave Hansen, an information technology systems analyst, wrote in a May 3, 1996, memorandum circulated to top executives and the chief lawyer for Metromail, which had $281 million in revenues last year and has budgeted $1.5 million to fight the case. The memo was one of the internal documents the company was recently required to turn over to the plaintiffs under discovery rulings by a state court in Travis County, Tex.

The company dossier on Ms. Dennis illustrates a central issue in the privacy debate: Information collected in one context can be reused in entirely unanticipated and even hostile ways without the knowledge or consent of the individuals involved. United States law offers them little recourse.

The Supreme Court has recognized an unwritten right to privacy in the Constitution, but has essentially limited this right to the individual's "reasonable expectation" of privacy. That approach, privacy experts say, means the steep but silent erosion of privacy by technological and economic change keeps narrowing the right to protection that an individual can successfully claim in court as "reasonable" — especially since privacy is weighed against competing interests, like law enforcement or freedom of the press. And like the unwritten constitutional right to privacy, most of the nation's patchwork of privacy legislation aims to protect individuals from government, not from the actions of private industry.

Metromail maintains in court that it did nothing wrong and that Ms. Dennis has no reasonable claim to privacy because she disclosed the information herself in consumer surveys. The company, a leading member of the Direct Marketing Association that champions industry self-regulation, calls the case an aberration, and adds that it no longer uses prison labor.

Because of the case, Texas is considering a complete ban on data entry by prisoners, but inmates in at least 27 other states handle public records like motor vehicle registrations, and Federal prisoners do such work for the Internal Revenue Service, among other public agencies. Prisons in at least five states reported contracts to process information for private businesses.

Public records are part of Metromail's information products. Its offerings include a "Behaviorbank" line that, for 4 cents to a quarter a piece, sells names, addresses and personal characteristics of respondents like Ms. Dennis to a wide assortment of clients, from direct marketers, bill collectors and reporters to politicians. Metromail customers include the marketing departments of major magazines and newspapers, including The New York Times.

Four new plaintiffs recently joined the class action by name after their information showed up in records that the lawsuit forced from Metromail and its subcontractor, Computerized Image and Data Systems in Roslyn Heights, N.Y., which sent the work to the prisoners. Like Ms. Dennis, the new plaintiffs said they felt tricked by surveys headlined, "Spending Too Much. You Can Save Money At the Supermarket," or "No sweepstakes, no promises, no gimmicks. Just FREE coupons, samples and other special offers." The outrage they expressed goes well beyond the prisoners' access to such data.

One, Edward Boslet, a 36-year-old meatcutter turned home health care technician in Plattsburgh, N.Y., summarized what to him is the heart of the matter.

"It's my information, it's not theirs," Mr. Boslet, a father of three, said in a telephone interview. "The bottom line is, I should have a right to know. I should have a right to choose who they're going to sell it to and what list I'm going to be on. There should be some way to govern what they do."

His convictions are not so far from the principles of fair information practice adopted by the European Union. But they are far from policy or practice in the United States.

Many people, especially in business, feel that is all to the good. They credit an unrestrained market in personal information as one reason for the United States' lead in the information economy.

"It's beneficial to the economy, it's beneficial to consumers," said Chet Dalzell, a spokesman for the Direct Marketing Association, the main trade group that is a longtime proponent of letting the industry regulate itself on privacy issues. Because the market can decide how to use personal information, he said, consumers get competitive offers of goods and services that are timely and relevant to their own lives, while businesses save on marketing costs.

"This isn't a war," Mr. Dalzell added. "This is the marketplace just trying to be intelligent." A recent study that the association commissioned from Ciemax-WEFA, an economics consulting company, said one of every 13 jobs in the United States is the result of direct marketing sales activity, including jobs designing and selling advertising, supplying or delivering goods, and selling other support services, like customer lists and profiles, to direct-response businesses. Direct-marketing sales to consumers reached $630 billion last year, up from $458 billion in 1991. Business-to-business sales were $540 billion in 1996, up from $349 billion in 1991, according to the Ciemax-WEFA report.

In other sectors, from health care to welfare, the ever more intensive use of personal information is being embraced as a way to cut costs and improve outcome, whether through employee "wellness" plans that discourage unhealthy life styles, or through child-support enforcement programs that combine public and private sector data bases to find parents who are delinquent in child support payments.

But incidents like these across the country offer glimpses of the less visible trade-offs:

¶At a car dealership in northern New Jersey, 15 employees used the company's access to the Big Three credit bureaus —

FOCUS ON YOUR HEALTH

PRIVACY

Naked Before the World

Will your medical secrets be safe in a new national databank?

BY ELLYN E. SPRAGINS AND MARY HAGER

WHOM, EXACTLY, DO YOU WANT TO know about your heart defect? Your family's history of breast cancer? Or that embarrassing brush with venereal disease 15 years ago? If you're like most people, you wouldn't be eager to give such information to a prospective boss or health insurer. Soon you may not have a say in the matter.

Your secrets are well on their way to becoming common knowledge, readily summoned by a few computer keystrokes. An alarming array of companies is already busily culling information from consumers' medical records. And a little-noticed section of the Health Care Portability and Accountability Act that passed last year could make it even easier for all kinds of strangers to find out if you've ever had an abortion or if depression is keeping you glued to your bed in the morning. "What this means is that whatever medical information is collected on people can be used for or against them, depending upon who asks for it," says Rep. Jim McDermott of Washington.

On the face of it, the new law is simply moving medicine into the computer age. It calls for standardization of all the bits and pieces of medical information compiled by doctors, hospitals, health plans and insurers about their patients. There's no end to the benefits of uniformity, say backers. First, patient data will flow electronically among insurers and health-care providers, making it cheaper to track and pay claims. Electronic links among health-care groups will make it easier for an emergency-room doctor, for example, to quickly call up a patient's medical history. Researchers and statisticians will have acres of compatible data to pore over. The network will even help the police finger suspects.

But all this good-for-you progress is marred by one big, ugly fact: every detail of your medical profile may in this new system without your consent. How could such a violation of doctor-patient confidentiality happen? Easy. "There's no law protecting consumers' medical records," says Lewis Maltby, a staff director at the ACLU.

Hospitals and doctors are already beginning to record their notes in electronic

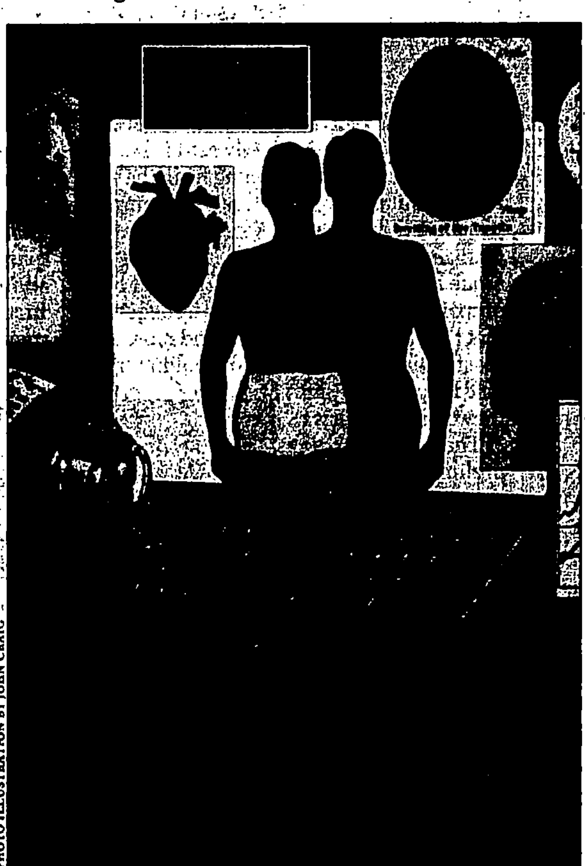


PHOTO ILLUSTRATION BY JOHN CRAIG

form. Once the new, linked system is in place, their disparate chronicles will form a national databank. Anyone who knows your special health-care number will be privy to some of your most closely guarded secrets. Already, managed-care companies demand details from psychotherapists' sessions. "Almost no one understands the depth of information being collected," says Denise Nagel, founder of the National Coalition for Patient Rights, in Lexington, Mass. The National Committee on Vital Health Statistics tentatively recommended that this mother lode of medical information be further augmented by specifics on living arrangements, schooling, gender and race.

As it stands now, insurers and others can't lay their hands on your records unless you sign a release. In many states they need special permission to get sensitive information, such as your HIV status or mental-health record. But there's no certainty that you'll have similar control under the new system. Organizations clamoring for unfettered access to the databank include insurers, self-insured employers, health plans, drugstores, biotech companies and law-enforcement agencies.

What will safeguard our secrets in this Orwellian project? Good question. The law does require Congress to enact privacy legislation. But no one seems to have confidence that protective shields will work. "If the CIA had its Web site invaded by vandals, how secure is this database going to be?" asks Donald Palmisano, the American Medical Association's spokesman on privacy issues.

Take some steps to protect your privacy. First, know what's actually in your medical record. Request a copy of your record from the doctors and hospitals that treat you, or go to the records department and take a look. Also, be sure to date any release of medical information that you sign. Add an expiration date if one isn't specified on the form.

Guarding your future electronic record will be a bit harder. You can call the National Coalition for Patient Rights (888-44-PRIVACY) to register your name on a pro-privacy petition that suggests consumers control who sees their medical information. And it's also smart to lobby your employer's benefits department. Since corporate employers are the health-care world's big spenders, their opinions really count. Now's the time to voice your opinion loudly. Otherwise your health secrets could quickly become an open book. ■