

1 of 1 DOCUMENT

Copyright 1997 The New York Times Company
The New York Times

June 12, 1997, Thursday, Late Edition - Final

SECTION: Section A; Page 1; Column 1; National Desk**LENGTH:** 6257 words**HEADLINE:** LIVES ON FILE: The Erosion of Privacy — A special report.;
Personal Files Via Computer Offer Money and Pose Threat**BYLINE:** By NINA BERNSTEIN**BODY:**

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: health care, entertainment, banking and supermarket sales. It is being 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 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, whether direct marketers, bill collectors, reporters and 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 meat-cutter 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 was 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 — Equifax Inc., Trans Union and TRW Inc. — to find strangers with good credit histories, living as far away as Alaska and Washington. They opened 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 Munsen, 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.

The New York Times, June 12, 1997

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, 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 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 Metromail's 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 money to the Department of Corrections.

Problems in the past had included obscene "nasty-grams," inserted at random by prisoners stuffing envelopes for the Texas tourism department, and 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 position of the gas meter on each parcel. Aerial photographs of the city of Bryan, Tex., 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 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 with 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 the tax assessment, the occupant's driver's license photograph and 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 pre-industrial 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 appeared on her computer screen. Ms. Dennis was monitored electronically as she followed a script demanding payment for things as diverse as Apple Macintosh computers and 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 also 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 turned my whole life upside down."

GRAPHIC: Photos: A Texas woman's answers to this 77-question consumer survey ended up in the hands of felons. (pg. A1); At the Ferguson state prison near Midway, Tex., inmates use a cutting-edge technology to put detailed maps and aerial photographs into computerized form. At the Texas prison in Huntsville thousands of boxes of public records were processed before the business moved to another prison. (F. Carter Smith for The New York Times)(pg. B14); 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. (Tony Dejak for The New York Times); 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. (Karen van Donge/The Arkansas Democrat-Gazette)(pg. B15)

Chart: "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

ACTIVITY: Joe calls an 800 number to check the pollen count.

DATA CAPTURE: Joe's number is caught through Caller ID; his name and address are pulled from a public records data base.

FIRST USE: Joe is put on a list of allergy sufferers; it is sold to a drug company marketing allergy pills.

LATER USE: The list is linked with a profile of Joe and he is sent a coupon for the company's allergy medication.

Driving

ACTIVITY: Rushing to work, Joe inadvertently runs a red light.

DATA CAPTURE: Though the intersection is empty, a video camera captures his license number.

FIRST USE: Joe is sent a traffic ticket in the mail.

LATER USE: Joe's insurance company finds the violation in a data base search and raises his rates.

Sending E-mail

ACTIVITY: At work, Joe criticizes his boss in E-mail to a friend.

DATA CAPTURE: Joe's company reviews employee Internet activity and keeps copies of all E-mail.

FIRST USE: After Joe's boss reads the E-mail, Joe is dismissed.

LATER USE: Joe's unsuccessful lawsuit to regain his job shows up when a prospective employer uses an Internet investigation service.

Dining

ACTIVITY: Joe eats lunch at a restaurant that records each order on a computer.

DATA CAPTURE: Joe pays by credit card, linking his account number to his order of a bacon cheeseburger and fries.

FIRST USE: The restaurant checks his credit standing and sends him a discount offer.

LATER USE: The restaurant goes bankrupt and its list of men who are bacon cheeseburger lovers goes on the information market.

Getting Prescriptions

ACTIVITY: Joe stops at the pharmacy to fil a tranquilizer prescription.

DATA CAPTURE: His name, the drug and his doctor become part of the data base of the pharmacy chain.

FIRST USE: The chain is part of a pharmaceutical company that combines the data with lists of magazine subscribers.

LATER USE: A rival tranquilizer company advertises in Joe's favorite magazine; company mailings urge Joe's doctor to switch.

Shopping

ACTIVITY: At the supermarket, Joe uses a discount shopper's card.

DATA CAPTURE: The card links Joe's identity to every item he buys.

FIRST USE: The supermarket chain uses a data-mining service to create profiles of its most profitable customers.

LATER USE: Joe is deemed a prized customer and gets electronically-generated discounts; less loyal customers pay more.

Mail Ordering

ACTIVITY: Before bed, Joe orders cufflinks and silk boxer shorts from a catalogue.

DATA CAPTURE: He pays by American Express, which adds his name to lists of buyers of expensive jewelry.

FIRST USE: The catalogue company puts his name on a list of male buyers of sexy lingerie and trades it with other companies.

LATER USE: Within two weeks Joe will receive four jewelry catalogues, five lingerie catalogues and a sex-videotape offer. (pg. B15)

LOAD-DATE: June 12, 1997