

The evidence presented in the following pages points to a conclusion that is both obvious and often ignored, namely, currently the main danger to privacy for people who live in free democratic societies comes from the private sector, not the government; Big Bucks, not Big Brother. This is highlighted by the sources of systematic authorized abuse of personal information, as distinct from occasional unauthorized use of such information by some rogue employee or merchant; it is further supported by an examination of the line-up of those who oppose new measures seeking to protect privacy in general and medical privacy in particular.

Progressive people long have viewed the government as the enemy of privacy. It has been shown that in the Edgar Hoover age, the FBI and local police forces often opened the mail and tapped the phones of civil rights leaders and anti-war activists. The ACLU protests programs of mandatory drug testing and searches of school lockers by local authorities. Cyber-libertarians vigorously object to government demands to obtain "keys" to privately encrypted messages. Above all, privacy--like our other basic rights--defends individual liberty from the government. In recent years, though, privacy has been not so much diminished as stripped away by privacy merchants, who make a hefty profit selling privacy-violating information.

Privacy Merchants

Privacy merchants come in two basic varieties: One comprises those corporations that specialize in this area, those whose only line of business is gathering and marketing personal information (not to be confused with statistical information that deals with groups of people but as a rule does not enable the buyer to violate the privacy of those encompassed). Major privacy merchants are Trans Union, Equifax, and Experian, which keep tabs on the credit histories (including addresses and Social Security numbers) of millions of Americans. Indeed, these three corporations are reported to maintain files on more than 90% of adult Americans.

The second category encompasses corporations that collect personal information about their own clients and use it either for their own marketing (e.g., Amazon.com), or sell it to others for their marketing purposes (e.g., NationsBank, LL Bean, Macy's, FTD florist). These corporations often use technological devices known as "cookies" that are planted on one's hard drive to allow the website owner to track sites visited, purchases made, and other information. Cookies allow marketers to recognize a person's computer when its operator approaches them again, and to tailor advertising to that person. Some ask the permission of their customers to collect information about them; many do not.

I first stumbled upon privacy merchants when I started editing a quarterly journal, *The Responsive Community*, about the same time as *American Prospect* was launched. Like other magazine publishers I purchased lists of subscribers to existing publications from list brokers such as the American List Council, Metromail, and Database America. These lists were then used to solicit people to subscribe to our publication. Aside from adding a bit to their junk mail, I must admit I did not realize at the time that I could have used the same lists to find out who subscribes to far right, far left, or pornographic magazines.

There are more than 30,000 commercially available lists on every conceivable kind of things people purchase or do in North America, profiling more than 100 million businesses and consumers, according to Edith Roman Associates, a names list broker.

List Brokers, Inc. of San Antonio maintains homeowner lists containing millions of records pertaining just to the state of Texas. The lists contain information on the age of the home, square footage, age of the occupant(s), and whether the occupant(s) is married or single. The company's "occupant lists" of deliverable residence addresses also contains income level.

Three major corporations that administer prescription data in the US are PCS Health Systems, owned by Eli Lilly & Co., Merck-Medco, and Diversified Pharmaceutical Services, a SmithKline Beecham company. These companies use patients' prescription and personal data to market drugs, for example, to urge doctors to switch their patients to drugs these companies sell or to advertise drugs directly to consumers so that they will ask their doctors about them by name. Merck-Medco covers more than 51 million people and manages more than 291 million prescriptions for clients. PCS Health Systems covers approximately 56 million people, and maintains a database of 1.5 billion prescriptions.

CMG Information Services maintains a product/service called Engage. Several large commercial sites on the World Wide Web have agreed to feed information about their customers' reading, shopping, and entertainment habits into the Engage system.

Other privacy merchants either collect massive amounts of information on potential customers or purchase it from other companies, including details on where a person travels, with whom (secretary?), places the person frequents (massage parlor?), what medications the person purchases (Antabuse?), and so on. One can also buy, from various websites, detailed accounts of individuals' stock holdings, account balances, and other financial information. The information is sold to debt collectors, private investigators, and anybody else who will foot the bill.

The costs are not a great burden: \$190 to uncover stock, bond, and mutual fund holdings; \$450 to reveal a credit card number; between \$80 and \$200 to provide telephone records; \$400 for access to 10 years' medical history, and between \$10 and \$20 to buy a divorce, death claim, fictitious name, or bankruptcy search.

If any details are missing, they can easily be filled in. A private investigator researching a claimant in a lawsuit against her employer "generated a five-page computer print-out from her name alone." The private eye found her Social Security number, date of birth, every address where she had ever lived, the names and telephone numbers of past and present neighbors, the number of bedrooms in a house she had inherited, her welfare history, and the work histories of her children's fathers.

Violations of Medical Privacy

Some Americans may feel that they care little if everyone knows their shoe or hat size, although they may discover that the size of their waistline may limit their employment opportunities. But few will react in such a nonchalant way when they discover that their medical privacy is violated with about the same impunity by the same privacy merchants as are the rest of their private affairs. In the following discussion, I focus on medical privacy as a kind of a domino-effect test; if the forces that violate the privacy of our medical records cannot be stopped, they are unlikely to be stopped elsewhere.

The media often plays up isolated cases of unauthorized use of medical information, in the tradition of individualizing our social problems and, at least inadvertently, distracting attention from their social sources. For instance, the press reported that a database created by the state of Maryland in 1993 to keep the medical records of its residents was used by a banker to call in the loans of his customers whom he discovered had cancer. While visiting her mother at the hospital at which she worked, the 13-year-old daughter of a nurse walked up to a computer terminal and accessed the hospital's online patient files. The girl then used the information to call female patients and tell them they were infected with the HIV virus or were pregnant. After receiving such a call, one teenage victim tried to obtain her father's gun to commit suicide before being stopped by her family. A medical student in Colorado sold the medical records of patients to malpractice lawyers who were looking for promising cases. When Nydia Velazquez was running for Congress in 1992 to represent New York City's 12th Congressional District, someone obtained hospital records detailing her 1991 suicide attempt and forwarded them to the press. The *New York Post* published the story, forcing Velazquez to acknowledge publicly something even her family did not know: she had tried to kill herself with sleeping pills and vodka.

All these incidences of people's medical records being publicized, and many others that have been reported, have several attributes in common: typically they are isolated acts, often committed by a single person; they are, as a rule, in violation of the policies and ethical codes of the institutions in which they took place; and in some circumstances are in violation of federal or state laws. As troubling as these incidences of unauthorized use are, they pale in terms of the scope of the ill consequences resulting from what might be called "authorized abuse." The latter intrusions are new because they have become possible only with the massive introduction of electronic medical records, which are rapidly replacing paper records, and changes in insurance schemes in the HMO age.

Privacy-Diminishing Developments in the Cyber-Age

There has been a powerful trend in the US in recent years to gather and record greater and more detailed information in medical records, including genetic information and lifestyle details. The health insurance industry now collects much larger amounts of information from physicians than it gathered in the past, amassing very large databases of personal information. Until recently, insurance companies usually received only an abstract of a patient's record, containing information on diagnoses, tests performed, and treatment provided. Nowadays, it is not uncommon for insurers to demand to see a patient's entire record. The shift to managed care programs (run by HMOs) has generated considerable additional demand for detailed

patient information by groups other than doctors and other treating personnel. For instance, representatives of managed care companies have required psychiatrists, as condition for payment, to reveal considerable details about their patients to verify that treatment was necessary. One study found that 37 percent of respondents to a survey of psychologists and psychoanalysts by the Santa Clara County Psychological Association said they "had a client who either decided against therapy or interrupted it 'because of confidentiality concerns."

Equally important are technological developments, especially the move by health care organizations to switch the format of their medical information from traditional paper-based files to computerized records that are stored in online databases.

The increasing prevalence of electronic medical records has been compounded by moves to link health care databases. This, in effect, turns numerous databases into one. Such linking often takes place within a single entity, for example, hospitals, clinics, and outpatient services all located within one medical center. Of a greater order of magnitude are the linkages among discrete organizations that render personal medical information accessible to a large number of institutions with distinct purposes, such as pharmaceutical marketers, employers, research centers, and others.

Electronic medical records are also distinct from traditional paper-based records in the ease with which longitudinal records are created, forming what a congressional Office of Technology Assessment report terms "a cradle to grave view of a patient's health care history." One can easily imagine the difficulty of such an endeavor in the old paper-based system for a patient who has lived in several cities, and thus has records scattered among many physicians and hospitals that have no ties to one another and are in different locations. One can just as easily imagine the relative ease of compiling such information when the separate records are entered into online databases. As a result, there is no escaping earlier facts, from drug abuse as a teenager to family histories of mental illness. The great gains in efficiency of electronic systems have caused a very considerable loss of privacy.

Additional concerns are raised by the fact that once online, health information can be linked with other, non-health data sets, such as an individual's credit report, to create encompassing personal dossiers. In 1995, Equifax, the giant consumer credit reporting agency, announced it would supply computerized medical records systems in addition to consumer credit reports. Together, these personal data may be used by employers, private investigators, lawyers, or others who may have a non-beneficent interest in an individual's personal health or lifestyle, or most anything else.

As a result of all these developments, the prestigious Institute of Medicine, part of the National Academy of Sciences, concluded that said developments

raised numerous issues, including (1) worries on the part of health care providers and clinicians about use or misuse of the information health database organizations will compile and release, and (2) alarm on the part of consumers, patients, and their physicians about how well the privacy and confidentiality of personal health information will be guarded.

Authorized Abuse

Most violations of privacy of medical records are the result of legally sanctioned, or at least tolerated, unconcealed, systematic flows of medical information from the orbit of the physician-patient-health insurer and health management corporations to other, non-health care parties, including employers, marketers, and the press. I refer here not to the occasional slip-up or the work of a rogue employee, cases that often violate ethical codes or laws, but to the daily, continuous, and very numerous disclosures and usages that are legal but of highly questionable moral value and intent, acts that may be labeled authorized abuse.

One major problem area is the disclosure of information by some health insurance companies to employers, information which employers then use to the detriment of prospective or current employees. In 1996, 35 percent of the Fortune 500 companies acknowledged that they draw on personal health information in making employment decisions, in a survey conducted at the University of Illinois at Urbana-Champaign. These companies employ many millions of people.

Another example of authorized abuse is when corporations that self-insure (provide health insurance plans of their own to their workers) draw on their personnel departments or medical claims divisions for privacy-violating data. According to recent figures from the General Accounting Office and the Employee Benefit Research Institute, as many as 48 million people are involved. A 1991 survey by the Office of Technology Assessment found that one-third of employers used their personnel departments to examine the medical records of their employees, without notifying these employees.

Another avenue of employer access to personal medical information is exemplified by the Southeastern Pennsylvania Transit Authority (SEPTA). SEPTA had contracted Rite-Aid pharmacy to provide prescription benefits to its workers. The contract included a requirement for the pharmacy to provide SEPTA with systematic access to employees' prescription records. In one case, the supervisor of an employee was told that the employee was taking AIDS medication. While it is unclear to what use the information was put in this case, one can imagine how such data could be abused.

While information about people's genetic predispositions is collected much less often than other medical information, its collection is on the rise. Two-hundred and six cases of genetic discrimination against asymptomatic individuals were documented in a 1996 study conducted by Harvard and Stanford universities. The individuals involved suffered loss of employment, loss of insurance coverage, or ineligibility for insurance based on the genetic potential for disease--not on any current maladies or symptoms. In another survey, conducted jointly by several federal agencies, 550 people were found to have been denied jobs or health insurance due to genetic predisposition to certain illnesses. Nearly a third (31 percent) of members of families with inherited diseases were found to have been denied insurance coverage even though they displayed no symptoms, in a survey cited in congressional testimony by the director of the Human Genome Project, Dr. Francis Collins. It is safe to assume that there are numerous other cases, unrecorded, of people unaware of the reasons they were not hired, were fired, and so on.

Fear of improper use of medical records is harming medical research and may endanger treatment. On this topic, Senator Olympia J. Snowe reports:

One-third of high-risk women refused to participate in a Pennsylvania study to understand how to keep women healthy with a breast cancer gene. They refused to participate because they feared losing confidentiality with respect to genetic information. [At] the National Institutes of Health . . . 32 percent of women eligible to undergo genetic testing for a breast cancer gene refused to do so, again for fear of losing privacy and confidentiality with respect to genetic testing and genetic information.

Regarding treatment, A.G. Breitenstein, director of the Health Law Institute, an advocacy group based in Boston, said, "People are not going to feel comfortable going to the doctor, because now you are going to have a permanent record that will follow you around for the rest of your life that says you had syphilis, or depression, or an abortion or whatever else."

In addition to authorized abuse by employers, privacy merchants find that private medical information is a lucrative commodity. According to Kathleen A. Frawley, vice president of the American Health Information Management Association, "There is a whole market of people buying and selling medical information." One such marketing firm is IMS America of Totowa, New Jersey, which buys patient records--with personal identifying information attached--outright from state governments, medical clinics, and drug store chains.

The Medical Information Bureau (MIB) is a clearinghouse of personal medical information whose members include 680 life insurance companies and most major issuers of health and disability insurance in the US and Canada. Member companies are required to submit any information about the individuals they insure or who have applied for insurance that pertains to their life expectancy. This includes medical information, encompassing conditions such as high blood pressure and obesity, and other information that may affect insurability, such as a reckless driving record or participation in hazardous activities. Whenever an individual applies for health, life, or disability insurance, the company obtains the record MIB has compiled on him or her.

Pharmaceutical companies have obtained medical records to discover which prescription drugs individuals are using and which physicians are prescribing them, so that these companies may solicit the physicians to prescribe their drugs. These companies also obtain patient lists and medical information from pharmacists in order to advertise prescription drugs directly to select patients. Metromail, known for its National Consumer Database profiling approximately 92 million American households, maintains a medical database, Patient Select, containing 15 million names. For about \$.30 per name, large drug companies can pitch their products directly to angina sufferers, diabetics, or arthritics. CVS Corporation, the largest pharmacy chain in the Washington metropolitan area, and Giant Food, the largest grocery retailer in D.C. and surrounding areas, sent confidential prescription information to a database marketing and prescription tracking company, Elensys. Elensys used the data to send personalized letters to CVS and Giant pharmacy

customers, reminding them to follow their doctors' prescriptions and to refill their prescriptions. Elensys also arranged for pharmaceutical companies, such as Glaxo Wellcome, to pay the pharmacies for the right to send marketing materials to the pharmacies' customers.

All this sharing of information occurred *without* customers' knowledge or consent. George Lundberg, the editor of the *Journal of the American Medical Association*, called these arrangements "a gross violation" of privacy, wondering, "Do you want . . . the great computer in the sky to have a computer list of every drug you take, from which can be deduced your likely diseases--and all without your permission?" Notably, when Janlori Goldman, herself an authority on medical privacy, was pregnant she received by mail coupons for parenting magazines and baby merchandise. She never was able to find out how the marketers knew about her condition.

The opposition to reform

The opposition to measures to shore up privacy of personal medical information is led by major industry groups such as the Health Benefits Coalition, which has financed an advertising and lobbying campaign to stop the patient rights bill "dead in its tracks" and the Healthcare Leadership Council, comprising approximately 50 large pharmaceutical companies, trade groups, and managed care plans. The HLC, in fact, has hosted multiple meetings in the districts of Republican Members of Congress who support the patients rights bill to expose them to local leaders' complaints about the proposed legislation. The Health Insurance Association of America, along with the US Chamber of Commerce, the Blue Cross Blue Shield Association, and others, pledged to oppose any effort to legislate patient rights. And the \$1 billion-a-year data transaction industry, including companies such as IBM, MasterCard, and Electronic Data Systems fear that proposed new forms of data protection, included in the draft legislation, would complicate their work. As a result, like many other privacy-protecting acts before it, a proposed patients' bill of rights was not enacted in 1998.

Still, leading libertarians persist in their focus on the government as the great enemy to individual privacy. Writing about this issue (although without specific reference to medical records) in the libertarian publication *Reason*, Brian Taylor states, "While private-sector surveillance is commonplace and widely accepted . . . the trends of placing cameras in public areas for use by law enforcement is a new and disconcerting variation on the established practice."

Solveig Singleton stakes out this anachronistic position more starkly, in a Cato Institute report:

We have no good reason to create new privacy rights. Most private-sector firms that collect information about consumers do so only in order to sell more merchandise. That hardly constitutes a sinister motive. There is little reason to fear the growth of private-sector databases. What we should fear is the growth of government databases.

Writing about another form of threat to privacy, ID cards, the Coalition for Constitutional Liberties argues:

This plan pushes us to the brink of tyranny, where citizens will not be allowed to travel, open bank accounts, obtain health care, get a job or purchase firearms without first presenting the proper government papers. The authorizing section of the law and the subsequent NHTSA proposal is reminiscent of the totalitarian dictates of Politburo members in the former Soviet Union, not the Congress of the United States of America.

The line up is rounded off by Phyllis Schlafly, who states more directly what her somewhat more moderate partners imply:

Do you worry that Big Brother (a.k.a. the Federal Government) wants to monitor your phone calls, your e-mail, your computer files, your health and financial records, and your business--and even build government databases containing personal information about you, your activities, your medical treatment, and your finances? You should.

She continues:

Putting all that information on a government database means the end of privacy as we know it. Daily actions we all take for granted will henceforth be recorded, monitored, tracked, and contingent on showing The Card.

Allowing the government to collect and store personal medical records, and to track us as we move about in our daily lives, puts awesome power in the hands of government bureaucrats. It gives them power to force us to conform to government health care policy, whether that means mandating that all children be immunized with an AIDS vaccine when it is put on the market, or mandating that expensive medical treatment must be withheld from seniors.

Once all medical records are computerized with unique identifiers such as Social Security numbers, an instant check system will give all government agencies the power to deny basic services, including daycare, school, college, access to hospital emergency rooms, health insurance, a driver's license, etc., to those who don't conform to government health policies.

One should also note that public authorities that need information about a person could purchase it from the very ample private databases rather than snooping themselves. Indeed, this is far from a theoretical conjecture. The FBI has been seeking for several years the cooperation of corporations that operate cellular phones to pinpoint the location of callers. The companies refused, on privacy grounds, to develop such a capacity and to make it available to public authorities. The FTC has been reluctant to require the private companies to cooperate. Meanwhile, however, consumer demand for such location devices is developing, and soon all the FBI will have to do is stop by a Radio Shack or some other electronic device store to purchase the "Big Brother" tools it seeks.

Besides, if a totalitarian regime were to arise, the new secret police would have only to consolidate existing private databases to have a very elaborate description of most Americans. Some homeless persons and a few hardcore criminals, those who have never held a job or have always used false IDs, might escape detection for a while. But there would hardly be enough of them to slow down a determined despot. While

authorities in a democratic society are checked by the need for subpoena power, a totalitarian state would not bother with such niceties.

In sum, in what might be called the "privacy paradox," most civil libertarians and many other privacy advocates continue to point the finger at government as the enemy of privacy, despite massive evidence that privacy merchants are such a considerable threat right now, while at the same time these advocates have sought to stop massive and encompassing privacy violations by these profiteers by drawing on new *legislation*--that is, on the government.

What Is to Be Done?

One can relatively readily list measures that would enhance medical privacy a great deal. These include some new technological devices (for instance, audit trails that record the identity of everyone who accesses a file and scare away unauthorized users) and social arrangements (for example, audits conducted by e-trusts certifying that companies that gain their seal of approval do not violate privacy). And some new legislation is being drafted. Indeed, unless Congress acts by August 1999, Secretary of Health and Human Services Donna Shalala is required by law to promulgate new privacy legislation. However, the basic issue is political. Faced with strong lobbies representing privacy merchants, many attempts to improve privacy protection, especially via new government regulation, have faltered. The political matrix will change only if those concerned with enhancing privacy make such protections a major part of their agenda. And this will not occur until they cease viewing the government as the enemy of privacy.

This essay draws directly on the author's *The Limits of Privacy*, (New York: Basic Books, 1999).