CATO INSTITUTE BRIEFING PAPERS

Watching You
Systematic Federal Surveillance of Ordinary Americans

by Charlotte Twight

No. 69 October 17, 2001

To combat terrorism, Attorney General John Ashcroft has asked Congress to "enhance" the government's ability to conduct domestic surveillance of citizens. The Justice Department's legislative proposals would give federal law enforcement agents new access to personal information contained in business and school records. Before acting on those legislative proposals, lawmakers should pause to consider the extent to which the lives of ordinary Americans already are monitored by the federal government.

Over the years, the federal government has instituted a variety of data collection programs that compel the production, retention, and dissemination of personal information about every American citizen. Linked through an individual's Social Security number, these labor, medical, education and financial databases now empower the federal government to obtain a detailed portrait of any person: the checks he writes, the types of causes he supports, and what he says "privately" to his doctor. Despite widespread public concern about preserving privacy, these data collection systems have been enacted in the name of "reducing fraud" and "promoting efficiency" in various government programs.

Having exposed most areas of American life to ongoing government scrutiny and recording, Congress is now poised to expand and universalize federal tracking of citizen life. The inevitable consequence of such constant surveillance, however, is metastasizing government control over society. If that happens, our government will have perverted its most fundamental mission and destroyed the privacy and liberty that it was supposed to protect.

Charlotte Twight is a professor of economics at Boise State University, a lawyer, and the author of Dependent on D.C.: The Rise of Federal Control over the Lives of Ordinary Americans *(Palgrave/St. Martin's, January 2002), from which this is excerpted.*

The outgrowth of all-encompassing federal collection of personal information is increased government power and concomitant individual dependence on government.

> When a large part of the information about economic statistics or administrative arrangements is collected and issued by the government, investigators and critics are forced to approach the very officials they may criticise for the information that might give substance to their criticisms.
>
> H. B. Acton (1971)[1]

Dependency's Forgotten Vector: Government-Compelled Information

Imagine for a moment a nation whose central government mandated ongoing collection of detailed personal information—individually identified—recording each citizen's employment, income, childhood and subsequent educational experiences, medical history (including doctors' subjective impressions), financial transactions (including copies of personal checks written), ancestry, living conditions (including bathroom, kitchen, and bedroom facilities), rent or mortgage payments, household expenses, roommates and their characteristics, in-home telephone service, automobile ownership, household heating and sewage systems, number of stillbirths, language capability—and periodically even demanded to know what time each person in the household usually left home to go to work during the previous week. Imagine further that such a government assigned every citizen a central government identification number at birth and mandated its use in reporting the information listed above. Suppose the same government were actively considering mandatory nationwide use of a "biometric identifier," such as fingerprints or retinal scans, along with a new counterfeit-proof permanent government identification card incorporating the individual's government-issued number and other personal information, encoded in magnetic strips and embedded computer chips capable of holding up to 1,600 pages of information about the individual. If a contemporary novelist were to portray the emergence of such a government in America, his novel undoubtedly would be regarded as futuristic fiction, in the same vein as George Orwell's *1984*.

Yet this national portrait is no longer fiction. The foregoing description is of a government that now wields exactly those ominous powers over the citizenry: America's federal government at the beginning of the twenty-first century. The logical outgrowth of such all-encompassing federal collection of personal information is increased government power and concomitant individual dependence on government. Altered political transaction costs again have supplied the means, with the information-collection authority described in this chapter emerging both as a product and instrument of transaction-cost manipulation.

Governments long have recognized information collection's capacity to erode individual autonomy by fostering deep personal uncertainty about the uses to which the information will be put. Law professor Paul Schwartz described this linkage clearly:

> Personal information can be shared to develop a basis for trust, but the mandatory disclosure of personal information can have a destructive effect on human independence. . . . Totalitarian regimes have already demonstrated the fragility of the human capacity for autonomy. The effectiveness of these regimes in rendering adults as helpless as children is in large part a product of the uncertainty that they instill regarding their use of personal information.[2]

With respect to U.S. government data collection in the 1990s, he added: "Americans no longer know how their personal information will be applied, who will gain access to it, and what decisions will be made with it. The resulting uncertainty increases pressure for conformity. Individuals whose personal data are shared, processed and stored by a myste-

rious, incalculable bureaucracy will be more likely to act as the government wishes them to behave." With extensive federal data collection creating ever greater incentives to behave as government wishes us to behave, the result is metastasizing government control. Indeed, Schwartz viewed the computer's ability to digitize personal information as offering "the state and society a powerful way to control the behavior of individuals."[3] The result—and often the purpose—is a profound erosion of individual autonomy.

This chapter focuses on existing central government data-collection programs that share one defining characteristic: they compel production, retention, and dissemination of personal information about every American citizen.[4] Their target is ordinary American citizens carrying out ordinary day to-day activities of life. Although these programs by no means constitute the whole universe of federal data-collection activity, today they are the government's most critical informational levers for institutionalizing government control, individual dependence, and unprecedented threats to cherished American liberties. Even within this circumscribed sphere, the immense volume of federal data collection defies brief summary. Accordingly, this chapter highlights the development and recent expansion of

- *Databases keyed to Social Security numbers*—examining unchecked use of Social Security numbers as a fulcrum for government data collection about individuals, and probing current legislative efforts to establish a national identification card;
- *Labor databases*—analyzing statutory provisions aimed at building a federal database of all American workers and requiring employers to obtain the central government's approval before hiring employees;
- *Medical databases*—assessing creation of a "unique health identifier" and implementation of uniform electronic databases of personal medical information nationwide as mandated by the 1996 Health Insurance Portability and Accountability Act (HIPAA);
- *Education databases*—revealing federal databases mandated by Goals 2000 and related 1994 education acts that establish detailed national records of children's educational experiences and socioeconomic status; and
- *Financial databases*—describing provisions of federal statutory law requiring banks and other financial institutions to create permanent, readily retrievable records of each individual's checks, deposits, and other financial activities.

These databases, linked by individuals' Social Security numbers, now empower the federal government to obtain an astonishingly detailed portrait of any person in America, including the checks he writes, the types of causes he supports, and even what he says "privately" to his doctor.

Of course, federal officials always provide an appealing reason for such governmental intrusion into our private lives, however inadequate the reason or unconstitutional the intrusion. As we have seen, they predictably use political transaction-cost manipulation in their effort to minimize resistance, increasing the transaction costs to private individuals of perceiving—and taking collective action to resist—governmental encroachments. There is always an asserted benefit to be obtained, a plausible cover story.

The ostensible reasons have been diverse. We have been told that government-mandated use of Social Security numbers in electronic databases will help to "reduce fraud"—tax fraud, welfare fraud, the usual litany. We have been told that requiring businesses to contact the government for approval before hiring anyone will help in "cracking down on illegal immigration." We have been told that forcing private physicians to record what we say to them in confidence will "reduce health care fraud," promote "efficiency," allow "better emergency treatment," make it "easier for the patient" to keep track of his medical records,

There is always an asserted benefit to be obtained, a plausible cover story.

and the like. We have been told that government tracking of what public school teachers record concerning our children will assist in students' selection of a "career major," enhance assessment of school courses, and facilitate identification of students needing help. We have been told that government requirements that banks keep microfilm copies of all the checks we write will "reduce white-collar crime" and "inhibit money laundering." Who could oppose such worthy goals unless he has something to hide?

The immense powers now exercised by the federal government have made these rationales inevitable. Having empowered the federal government to exert centralized control over far-flung human endeavors, most Americans want government officials to administer the programs effectively and responsibly. But doing so necessitates "reducing fraud" and "promoting efficiency" in the programs, legitimate objectives that often become chameleonic rationales that ultimately are invoked in the service of illegitimate ends. The pattern is unmistakable: with vast federal power comes vast federal surveillance, providing plausible cover for those seeking to further extend the central government's purview.

Political transaction-cost manipulation has framed the issue in other ways besides these appealing rationales. Indeed, the backdrop for this chapter's discussion is the ubiquitous political transaction-cost manipulation, described in earlier chapters, that facilitated passage of the statutes that originally authorized and gave rise to this data collection: the Social Security Act, the health care legislation, the education statutes, and the like. That history will not be repeated here. Instead, this chapter provides additional examples of political transaction-cost manipulation specifically involving the data collection aspects of those laws, focusing on their use to support the central government's accelerating quest for detailed personal data about each and every American citizen.

In some cases discussed below, the database maneuvers were deliberately obscured from public view, buried in what writer Claire Wolfe called "land-mine legislation" that people don't notice until they step on it.[5] In other cases Americans were encouraged to view new proposals piecemeal, a strategy that forestalled public perception of the confluent streams of nationwide government-mandated data centralization and their likely eventual result. Incrementalism again served activist policymaking. Information-law scholar Simon Davies judged the public's "greater acceptance of privacy-invasive schemes" in recent years to be in part a result of "[p]roposals . . . being brought forward in a more careful and piecemeal fashion," which may be "lulling the public into a false sense of security."[6]

Legislators and members of the popular press today seldom discuss the likely cost of government data centralization in terms of lost liberty.

Given that piecemeal progression, legislators and members of the popular press today seldom discuss the likely cost of government data centralization in terms of lost liberty. Perhaps "liberty" does not resonate so strongly or create as powerful an image for most people as "cracking down on illegal immigration" or "reducing health care fraud." Liberty, after all, is an abstraction whose concrete reality often is not appreciated until its opposite is experienced firsthand. Yet we ignore at our peril the long-cited "use of personal information systems by Nazi Germany to enable the identification and location of a target race."[7] Race-based government roundups of law-abiding citizens also occurred in America less than sixty years ago, similarly facilitated by government data collection. As Cato Institute policy analyst Solveig Singleton and others have reported, "In the U.S., census data were used to find Japanese-Americans and force them into camps,"[8] a historical reality that gives fresh meaning to a 1990 U.S. Census instruction stating that "It is as important to get information about people and their houses as it is to count them."[9] By 2002, however, events of the 1940s have become only a "vague memory"—and, except for the elderly, not a living memory at all.[10]

So today Congress proceeds apace. Having exposed most areas of our lives to

ongoing government scrutiny and recording, Congress now is working to expand and universalize federal tracking of law-abiding citizens' private lives. Concurrently, new developments in biometry are producing technologies that most observers concede "imperil individual autonomy" and pose "real threats to the fabric of contemporary society."[11] The next generation awaits the full flowering of these technologies and their availability to governments. Our privacy, our personal identity, our independence, and our freedom hang in the balance.

Linking Personal Records: A "De Facto National Identification Number"[12]

The Social Security number (SSN) has become a key to detailed government knowledge of our private lives. Even the secretary of the Department of Health and Human Services (HHS) has described American Social Security numbers as a "*de facto* personal identifier."[13] Kristin Davis, senior associate editor of *Kiplinger's Personal Finance Magazine,* described "the growing use of social security numbers as an all-purpose ID" as the "single biggest threat to protecting our financial identities."[14] Since the Social Security program's inception in the 1930s, when officials slighted public fears that identification of citizens for Social Security purposes implied regimentation, that reality has relentlessly emerged.

Federal officials long denied that SSNs would function as national identification numbers. They were supposed to be mere "account numbers" denoting an individual's "old-age insurance account" in which his "contributions" were set aside in a federal "trust fund" for his retirement. But expansion of SSN use came quickly, much of it ordered by the federal government. President Franklin Roosevelt began the process in 1943 by ordering that thereafter, whenever the head of any federal department or agency found "it advisable to establish a new system of permanent account numbers pertaining to individual persons," the department or agency "shall . . . utilize exclusively the Social Security Act account numbers" assigned pursuant to that act.[15]

The full impact of Roosevelt's order was not felt until computers became available. Gradual computerization made SSN-based record systems increasingly appealing throughout the 1960s. In 1961 the Civil Service Commission first ordered the use of SSNs to identify all federal employees. The Internal Revenue Service (IRS) began using SSNs as taxpayer identification numbers in 1962. Department of Defense military personal records were identified by SSN beginning in 1967; the SSN became the Medicare identifier in the 1960s. Thereafter SSN use spread unabated:

> By the 1970s, the SSN floodgates had opened fully. Congress in 1972 amended the Social Security Act to require the use of SSNs for identifying legally-admitted aliens and anyone applying for federal benefits. In following years, additional legislation required the SSN for the identification of those eligible to receive Medicaid, Aid to Families with Dependent Children ("AFDC") benefits, food stamps, school lunch program benefits, and federal loans.[16]

Moreover, the 1970 Bank Secrecy Act, discussed later in this chapter, required all financial institutions to identify customers by SSN and preserve detailed records of their customers' personal checks and other financial transactions.

The Privacy Act of 1974 did not stop the flood.[17] Although it purported to restrict federal dissemination of SSNs, it not only exempted existing federal SSN use that had been previously authorized by statute or regulation but also created a massive exemption allowing disclosure of personal information obtained by federal officials if the disclosure involved a "routine use" of the data. Two years later, utterly countermanding any

Our privacy, our personal identity, our independence, and our freedom hang in the balance.

notion of restricting SSN use and dissemination, Congress included in the Tax Reform Act of 1976 a provision that gave states free rein to use SSNs. It stated:

> It is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security account numbers issued by the Secretary for the purpose of establishing the identification of individuals affected by such law, and may require any individual who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number . . . issued to him by the Secretary.[18]

For approximately the first fifty years of the Social Security program, one did not acquire an SSN until beginning one's first job, usually around age sixteen. Today every child must acquire an SSN at birth or shortly thereafter.

Incrementalist policies continued to advance SSN use, as illustrated by the gradual introduction of requirements that Social Security numbers be obtained for young children. For approximately the first fifty years of the Social Security program, one did not acquire an SSN until beginning one's first job, usually around age sixteen. Today every child must acquire an SSN at birth or shortly thereafter. How did policymakers accomplish such a radical change? Much as one conditions dogs: a bit at a time—and always with a reward attached. First, Congress required in 1986 that every child claimed as a dependent on federal tax forms have an SSN by age five. Then in 1988 they reduced it to age two. Then in 1990 they reduced it to age one. Finally, in 1996, they passed a global requirement that an SSN must be presented for anyone of any age claimed as a dependent on any federal tax form. No SSN, no federal tax deduction.[19] In general, to obtain any federal benefit today, tax-related or otherwise, one must present the Social Security numbers of all parties affected.[20] To facilitate assignment of SSNs at birth, the federal government has financed state "Enumeration at Birth" programs to secure issuance of the numbers as a routine part of birth certificate registration, a process that is now operational in all fifty states.

A coordinated government effort now under way to require even greater use of SSNs will further centralize federal monitoring of all American citizens. Its elements include

- federal mandates attempting to regulate state drivers' licenses and birth certificates;
- federal "work authorization" databases covering all working Americans and keyed to SSNs;
- federal development of a "unique health identifier" for each American in implementing uniform electronic databases of private medical histories;
- federal implementation of education databases; and
- federal development and issuance of new "tamper resistant" Social Security cards, perhaps with biometric identifiers, viewed by many as precursor of the long-feared "national identity card."

The education, medical history, and work authorization databases are discussed separately below. First I shall discuss the driver's license, birth certificate, and tamper-resistant Social Security card provisions.

In 1997 an unprecedented federal assertion of control over state-issued drivers' licenses tested the limits of public tolerance for expanding federal control over traditional state functions. Although this particular statutory language was repealed two years later, similar provisions linger, and the episode highlights both the direction of current congressional efforts and how the game is being played.

The provision was buried in an omnibus bill, the 749-page Omnibus Consolidated Appropriations Act of 1997, which included the "Illegal Immigration Reform and Immigrant Responsibility Act of 1996" (the

"Immigration Reform Act") that contained the relevant language.[21] The key provisions began on page 716, sandwiched between a section entitled "Sense of Congress on Discriminatory Application of New Brunswick Provincial Sales Tax" and another entitled "Border Patrol Museum." So well concealed, the provisions were difficult to spot even if you already knew they were there.

Section 656(b) of the Immigration Reform Act dealt with "State-Issued Drivers Licenses and Comparable Identification Documents." The language made compliance with federal rules specifying characteristics for these documents mandatory without actually saying so. It simply prohibited federal agencies from accepting a state-issued driver's license for identification purposes unless it satisfied federal requirements. Instead of telling the states "you must," it made it nearly impossible for state residents to interact with the federal government if the state did not comply. This charade of voluntariness was buttressed by hard cash—grants to states "to assist them in issuing driver's licenses and other comparable identification documents that satisfy the requirements" issued by the federal government.

Compliance required the states to follow federal Department of Transportation (DOT) regulations specifying both the form of the driver's license and federally acceptable "evidence of identity" in issuing the license. Raising the specter of biometric identifiers, it required "security features" intended to "limit tampering, counterfeiting, photocopying, or otherwise duplicating, the license or document for fraudulent purposes and to limit use of the license or document by impostors." In addition, the statute mandated that in general the driver's license or other identification document had to include a social security account number "that can be read visually or by electronic means." States could avoid including the SSN on the license only by requiring "every applicant for a driver's license . . . to submit the applicant's social security account number" and "verify[ing] with the Social Security Administration that such account number is valid." Either way, the SSN was readily at hand—and easily cross-linked electronically to any alternative identifier a state might adopt. Proposed federal DOT rules implementing these provisions were published in 1998.[22]

But section 656(b) was short lived. On October 9, 1999, Congress passed a lengthy appropriations bill covering appropriations for the DOT and related agencies. The forty-second page of that legislation contained a single sentence, with no heading or other explanation, that stated in its entirety: "Sec. 355. Section 656(b) of division C of the Omnibus Consolidated Appropriations Act of 1997 is repealed."[23] Section 656(b) thus perished through the same transaction-cost manipulating strategies that had enabled its passage in 1997. Like other incrementally installed federal controls, however, it will no doubt rise again. And, as shown in the next section's discussion of the new-hire legislation, a similar driver's license measure appeared elsewhere in the Immigration Reform Act.

The other prong of current federal efforts to control state-issued identification documents entails regulation of the states' issuance of birth certificates. Enacted into law as sec. 656(a) of the same 1996 Immigration Reform Act, it has not been repealed. The tactic was the same, requiring that federal agencies could not accept birth certificates for official purposes unless the birth certificate complied with federal regulations specifying "appropriate standards for birth certificates."[24] Bribes followed in the form of grants to states to help them issue birth certificates that "conform to the standards" in the federal regulation. Federal grants also were authorized for states to help them develop the "capability to match birth and death records" and to finance related demonstration projects. An explicit objective was to "note the fact of death on the birth certificates of deceased persons." However fleeting, the sole federal concession was to "not require a single design" for birth certificates in all states and to allow state differences in the "manner and form" of storing

Federal agencies could not accept birth certificates for official purposes unless the birth certificate complied with federal regulations.

Data mergers and exchanges are not aberrations, and they are not limited to information about suspected criminals: they are a systematic policy tool of today's federal government.

birth records and producing birth certificates. The substance was another matter.

Perhaps the most ominous of Congress's innocuously titled "Improvements in Identification-Related Documents" required development of "prototypes" of a "counterfeit-resistant Social Security card."[25] Congress specifically mandated that the prototype card "shall employ technologies that provide security features, such as magnetic stripes, holograms, and integrated circuits." Integrated circuits? Integrated circuits open the door to biometric identifiers and the storage of vast amounts of personal data on each person's government-required Social Security card, a theme that recurred in government discussions of the "unique health identifier" for medical records.[26] And they are not just aiming these changes at new people entering the Social Security system. The statute required the Social Security commissioner and the comptroller general to study the "cost and work load implications of issuing a counterfeit-resistant social security card for all individuals over a 3, 5, and 10 year period."[27] These new cards "shall be developed so as to provide individuals with reliable proof of citizenship or legal alien status." Proof of citizenship? Federal officials have claimed that such a document is not a "national identification card" because—note well—we will not be required to carry it around with us at all times.[28] Not yet, anyway.

Despite all such protestations, the SSN is now at the heart of a vast array of government databases, and linkage of those separate databases occurs regularly despite periodic statutory lip service to individual privacy. It is all perfectly legal under the 1988 Computer Matching and Privacy Protection Act discussed later in this chapter. Privacilla.org reported in March 2001 that agencies covered by the act listed forty-seven such exchanges "from September 1999 to February 2001" alone, meaning that a "federal government agency quietly announce[d] a new plan to exchange and merge databases of personal information about American citizens" more frequently than "once every other week."[29] Among the listed data-sharing transactions were exchanges of personal information about all of us between

- The IRS and the Social Security Administration (SSA);
- The SSA and the Health Care Financing Administration;
- The Postal Service and the Department of Labor;
- The Justice Department and the Department of Veterans Affairs;
- The IRS and state social services agencies;
- The Department of Education and HHS; and
- The SSA and the state courts.[30]

These data mergers and exchanges are not aberrations, and they are not limited to information about suspected criminals: they are a systematic policy tool of today's federal government, extending far beyond the agencies covered by the Computer Matching and Privacy Protection Act.[31]

Consider exchanges involving the Social Security Administration (SSA). Its own regulations state that SSA officials "disclose information when a law specifically requires it," including:

> disclosures to the SSA Office of Inspector General, the Federal Parent Locator Service, and to States pursuant to an arrangement regarding use of the Blood Donor Locator Service. Also, there are other laws which require that we furnish other agencies information which they need for their programs. These agencies include the Department of Veterans Affairs . . . , the Immigration and Naturalization Service . . . , the Railroad Retirement Board . . . , and to Federal, State, and local agencies administering Aid to Families with Dependent Children, Medicaid, unemployment compensation, food stamps, and other programs.[32]

And, of course, the IRS. "Information" is

defined to mean "information about an individual" which "includes, but is not limited to":

> vital statistics; race, sex, or other physical characteristics; earnings information; professional fees paid to an individual and other financial information; benefit data or other claims information; the social security number, employer identification number, or other individual identifier; address; phone number; medical information, including psychological or psychiatric information or lay information used in a medical determination; and information about marital and family relationships and other personal relationships.[33]

Even without the SSA's much reviled on-line dissemination in 1997 of the agency's database of "Personal Earnings and Benefit Estimate Statement" information on Americans, making the data electronically accessible via the Internet to third parties without the subject individual's knowledge or consent, the SSA's broad regulatory power to transmit personal information to other government agencies seriously compromises individual privacy.

Concrete examples of the data linkages across government agencies are provided by the Aid to Families with Dependent Children (AFDC) program—now called Temporary Assistance to Needy Families (TANF)—and the Child Support Enforcement (CSE) program. In describing the effects of computerization of federal records, law professor Paul Schwartz stated that "AFDC has progressed from midnight searches of the welfare beneficiary's home to continuous searches of the beneficiary's personal data." Explaining "the enormous amount of information to which AFDC offices have access" and the "extensive data bases that are manipulated in administering the AFDC program," Schwartz added:

> From the Social Security Administration, AFDC receives access to the BENDEX [Beneficiary Data System] and SDX [Medicare eligibility and Supplemental Security Income payment] data systems. From the Internal Revenue Service, AFDC receives data relating to the tax interception and parent locator programs. Within state government, AFDC receives information from the Employment Security Division (worker's compensation and employment) and the Child Support Enforcement Unit (child support payments). AFDC offices also receive information about unemployment payments from other states.[34]

Over time the program's broad reach predictably has spawned increasingly intrusive data collection and data sharing in the name of curtailing welfare fraud.

A similar pattern is evident in the federal Child Support Enforcement program. As Schwartz has recounted, after the program's creation in 1974, parent locator services in every state were granted access to ever more government databases of personal information. Their use of the SSN passkey was authorized in 1976, when "Congress explicitly authorized the use of social security numbers in searches of federal and state data banks for information leading to the location of these delinquent parents of AFDC families."[35] Thereafter Congress gave the parent locator services access to IRS records and extended the data matching program to all families, making even non-AFDC families subject to "data matching and tax interception with the IRS." Schwartz quoted a state director of CSE as saying, "Some people would say that's Big Brotherism. Well, it is."[36] Every child support enforcement unit (CSEU) has access to all the AFDC data listed above as well as to the Federal Parent Locator database. That database in turn contains information from "the Social Security Administration; the Department of Defense; the Veterans Administration; the Motor Vehicle Bureau of the state in which the CSEU is located; the IRS, including 1099

TANF's broad reach predictably has spawned increasingly intrusive data collection and data sharing in the name of curtailing welfare fraud.

forms; and commercial credit bureaus. The parent locator also allows searches of state data bases, three states at a time."[37]

Pervasive government extraction of personal data that are stored and linked via compulsory use of SSNs is today's reality. As more and more Americans worry about the damage that Social Security numbers have inflicted on our privacy, the federal government responded with the Social Security Number Confidentiality Act of 2000. A reassuring title, indeed. But the substance of that statute only demonstrated the flagrant disregard for American citizens' privacy that has characterized federal officials' actions for decades. The new statute's sole purpose was to instruct the secretary of the treasury henceforth to "ensure that Social Security account numbers (including derivatives of such numbers) are not visible on or through unopened mailings of checks or other drafts" issued by the federal government![38]

Incrementalism, misrepresentation, hiding threatening measures in larger bills, and other forms of transaction-cost manipulation have spawned a system of linked federal databases that now make it virtually impossible for a person to opt out of, let alone actively resist, the federal government's monitoring of ordinary, law-abiding American citizens. As we move toward the equivalent of a national identity card tied to the ubiquitous SSN, the threat to privacy is clear. Although it will not be labeled a national identity card, Stephen Moore of the Cato Institute correctly stated in his testimony on a related bill that if it "looks like a duck, . . . quacks like a duck, . . . walks like a duck . . . [i]t's a duck."[39]

As we move toward the equivalent of a national identity card tied to the ubiquitous SSN, the threat to privacy is clear.

Tracking (and Preventing) Your Employment: "Illegal Aliens" and Other Excuses

A key aspect of the federal government's ongoing effort to establish the equivalent of a national identity card is its quest to obtain current, continually updated, detailed electronic data about where and for whom each individual in America is working. To overcome resistance to such federal surveillance, Congress has used several rationales. Recurrent excuses for increasing federal surveillance of every working American are

- controlling illegal immigration;
- locating absent parents who owe child support payments;
- preventing welfare fraud; and
- supporting workforce investment.

These purported rationales have become ritual incantations; once they are uttered, Congress expects a mesmerized citizenry to grant whatever liberty-curtailing federal powers Congress demands. So far the strategy has worked.

During the 1990s federal authority to collect labor-related data skyrocketed. The federal government's desires were particularly evident in a 1992 amendment to the Job Training Partnership Act that ordered the commissioner of labor statistics, cooperating with state governments, to "determine appropriate procedures for establishing a nationwide database containing information on the quarterly earnings, establishment and industry affiliation, and geographic location of employment, for all individuals for whom such information is collected by the States," including "appropriate procedures for maintaining such information in a longitudinal manner."[40]

Four years later, further statutory changes supported these ends. The first was part of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, the 1996 welfare reform act.[41] For the stated purposes of preventing welfare fraud and enforcing child support obligations, the law established "Directory of New Hires" electronic databases at both the state and the national level, simultaneously authorizing pervasive new data sharing among federal and state agencies. Despite the law's welfare motif, neither the state nor national directories are limited in any way to individuals receiving public assistance or paying or receiving child support. Instead, these new databases

cover every working individual in America who enters the workforce or changes jobs.[42] Journalist Robert Pear has called it "one of the largest, most up-to-date files of personal information kept by the government" whose size and scope "have raised concerns about the potential for intrusions on privacy."[43]

The 1996 law specifies that each state must establish a State Directory of New Hires that "shall contain information supplied . . . by employers on each newly hired employee." Each employer is mandated to turn over to state officials "a report that contains the name, address, and social security number of the employee, and the name and address of, and identifying number assigned under . . . the Internal Revenue Code [to] the employer."[44] State officials then must give this information, along with wage and unemployment data on individuals, to the federal government for inclusion in its National Directory of New Hires. As *Forbes* writer Brigid McMenamin stated, "The new-hire legislation is one of dozens of federal and state laws that force U.S. employers to moonlight as unpaid police, nannies and tax collectors."[45] Within each state, the State Directory of New Hires must be matched against a mandatory "state case registry" containing "standardized data elements for both parents (such as names, social security numbers and other uniform identification numbers, dates of birth, and case identification numbers), and . . . such other information . . . as the Secretary may require."[46]

SSNs provide the key link between the electronic databases. State agencies are required to "conduct automated comparisons of the social security numbers reported by employers . . . and the social security numbers appearing in the records of the State case registry" to allow state agencies to enforce child-support obligations by mandatory wage withholding. States also are ordered to require SSNs of applicants for any "professional license, commercial driver's license, occupational license, or marriage license" and to include SSNs on certain court orders and on death certificates. Broad information sharing with other state and federal agencies and with "information comparison services" is mandated. Access to the new hires database is granted to the secretary of the treasury (IRS), and the SSA is to receive "all information" in the national directory. The statute instructs the secretary of HHS and the secretary of labor to "work jointly" to find "efficient methods of accessing the information" in the state and federal directories of new hires.[47]

Other major changes in 1996 came via the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. Although its most ominous provisions were cast as pilot programs, their scope and structure clearly indicated the direction of things to come. Using the rationale of controlling illegal immigration, this 1996 statute established pilot programs requiring employers to seek the central government's certification of a person's "work authorization" before finalizing an offer of employment. The manner in which the federal government's approval must be sought substantially overlaps the pressure for SSN-based national identification cards and enhanced SSN-based state drivers' licenses discussed earlier.

Congress created three "pilot programs for employment eligibility confirmation": the "basic" pilot program, the "citizen attestation" pilot program, and the "machine-readable-document" pilot program. Underlying all three was Congress's mandate that the U.S. attorney general establish a pilot "employment eligibility confirmation system," keyed to information provided by the SSA and the Immigration and Naturalization Service (INS). The idea is to create a federal database capable of confirming any individual's SSN and his INS-decreed work eligibility before an employer finalizes the hiring of that person. Prior to passage of the pilot program law, John J. Miller, vice president of the Center for Equal Opportunity, and Stephen Moore of the Cato Institute described such proposals as follows: "In other words, the government would, for the first time in history, require

Although the most ominous provisions of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 were cast as pilot programs, their scope and structure clearly indicated the direction of things to come.

employers to submit all of their hiring decisions for approval to a federal bureaucrat."[48] Although individual firms' election to participate was voluntary, the reward for participating was protection from both criminal and civil liability for "any action taken in good faith reliance on information provided through the confirmation system."[49]

The three pilot programs show that a national identification card system is coming ever closer. The "basic" program instituted a system of federal government confirmation of work eligibility. When hiring, recruiting, or referring any individual, participating firms must obtain the potential employee's SSN, or INS identification number for aliens, and require presentation of specified identification documents. The firms then must use the government's "confirmation system" to get federal approval for the hiring decision. The statute required that, within three working days after hiring a person, the employer "shall make an inquiry . . . using the confirmation system to seek confirmation of the identity and employment eligibility of any indiviual."[51] If the firm continues to employ the individual after a "final nonconfirmation" of work eligibility through the federal electronic database system, penalties of $2,000 to $10,000 per unauthorized hire may be imposed.[52]

With the citizen attestation pilot program, linkages with other parts of the coordinated federal data expansion effort became apparent. While extending the approach of the "basic" pilot program, the idea here is to waive the requirement for work eligibility confirmation in certain circumstances if the job applicant claims to be a U.S. citizen—but only if the state in which a participating firm is located has adjusted its *drivers' licenses* to include "security" features such as those described in the previous section. The statutory language is almost identical to that of the repealed sec. 656(b), requiring each state driver's license to contain both a photograph and "security features" that render it "resistant to counterfeiting, tampering, and fraudulent use."[53] If a state has complied with the federally desired format and application process for state drivers' licenses, then participating firms can avoid mandatory use of the federal work eligibility confirmation system by inspecting the job applicant's state driver's license.

The machine-readable-document pilot program came even closer to a national identity card approach. For firms to participate in it, their state must have adopted a driver's license format that includes a "machine-readable social security account number." Participating firms then "must make an inquiry through the confirmation system by using a machine-readable feature of such document" to obtain confirmation from the federal government of the work eligibility of new employees.[54] The potential for future linkage of such procedures to the new skill certificate programs called for by the 1994 School-to-Work Opportunities Act is all too evident.

After establishing the infrastructure for a national identification card, the 1996 Immigration Reform Act, like other recent statutes, included a provision headed "No National Identification Card," which proclaimed that "[n]othing in this subtitle shall be construed to authorize, directly or indirectly, the issuance or use of national identification cards or the establishment of a national identification card."[55] Such provisions, appearing ever more frequently in federal legislation, merely highlight the clear and present danger of exactly the type of system disavowed. Given this brazen political transaction-cost manipulation, we should take the advice of the newspaper comic strip character Cathy, who, after hearing her mother repeatedly state that she did not want any popcorn, delighted her mother by buying her a box of popcorn. Cathy explained to her astonished boyfriend that in her family it was important to "pay attention to the nouns," not the verbs and adverbs.[56] As Congress repeatedly insists that it has no interest in national identification cards, we would be well advised to start paying attention to the nouns.

Firms must use the government's "confirmation system" to get federal approval for hiring decisions.

A bill introduced in 1997, H.R. 231, reflected the continuing congressional pressure to move the nation closer to a national identification card system. Like the pilot program legislation, H.R. 231 prominently displayed a provision entitled "Not A National Identification Card." Further embracing the spirit of political transaction-cost manipulation, H.R. 231 was appealingly labeled as a bill "To improve the integrity of the Social Security card and to provide for criminal penalties for fraud and related activity involving work authorization documents for purposes of the Immigration and Nationality Act." Testifying before Congress on this bill, Stephen Moore described it as a dangerous extension of pilot work-authorization programs that had already created "an insidious national computer registry system with the federal government centralizing work authorization data on every one of the 120 million Americans in the workforce." Moore told the House Judiciary Committee's Subcommittee on Immigration and Claims:

> The centralized computer registry system is dangerous enough. But to add to that a photo i.d. card issued to every citizen that matches up with the computer data base is to put in place the entire infrastructure of a national i.d. card system. All that is missing is the nomenclature. As someone once put it: this is about as ill-fated as giving a teenager a bottle [of] booze and keys to a motorcycle, but getting him to promise that he won't drink and drive. You're just asking for trouble.[57]

We have already asked for trouble. With laws now on the books, we do have a national ID-card system; the real question is how much additional personal information we will pour into it.

Vastly more was poured into it in 1998. The Workforce Investment Act (discussed in Chapter 5) specifically authorized the secretary of labor to "oversee the development, maintenance, and continuous improvement of a nationwide employment statistics system" intended to "enumerate, estimate, and project employment opportunities and conditions at national, State, and local levels in a timely manner." Designed to include information on all of us and our employment, this system is to document the "employment and unemployment status of national, State, and local populations" and incorporate "employment and earnings information maintained in a longitudinal manner." Despite requirements for the data's "wide dissemination," the statute reassured us that this vast array of information would remain "confidential."[58]

Behind nomenclature that continues to conceal more than it reveals to ordinary Americans, government pressure thus persists for an ever increasing repository of personal information to fatten and consolidate national employment databases and identification systems. It is hard to disagree with McMenamin's judgment that "[t]he endgame is a single system rigged to keep track of everything about each employee, from résumé through pension plan, and to calculate every item to the last penny, and spit out all of the required reports on schedule."[59] The Workforce Investment Act and the federal pilot work-authorization program were steps in that direction, steps likely to be validated regardless of their actual effects. As Moore remarked regarding the work-authorization program, "It is almost a certainty that no matter how big a failure this new system proves to be, within ten years the registry will be applied to all workers in the nation."[60] Talismanic objectives such as controlling illegal immigration, enforcing child support obligations, and supporting workforce investment continue to provide fertile ground for rationalizing increased government surveillance of the employment and whereabouts of every person in America.

Tracking Your Personal Medical History: The "Unique Health Identifier"

Further jeopardizing our privacy and individual autonomy is the 1996 federal mandate

With laws now on the books, we do have a national ID-card system; the real question is how much additional personal information we will pour into it.

Federal officials plan to link and merge the databases virtually at will so as to accomplish whatever degree of centralization of personal medical information the government desires.

(discussed in Chapter 6) for a unique nationwide health identifier for each individual to be used in standardized electronic databases of personal medical information. Federal officials are quick to point out that they are not planning a single national database of such information. But what they do intend is to create the functional equivalent of such a database. Once the formats are standardized and identifiers specified, they plan to link and merge the databases virtually at will so as to accomplish whatever degree of centralization of personal medical information the government desires. Indeed, a federal report entitled "Toward a National Health Information Infrastructure" so stated, noting that "[c]urrently, health information is stored in many locations," but the "NHII [National Health Information Infrastructure] seeks to connect that information where links are appropriate, authorized by law and patient permissions, and protected by security policies and mechanisms."[61] As we saw in Chapter 6, the central government used similar language in HIPAA privacy regulations that actually reduced privacy—authorizing broad access to medical records by government agencies without patient consent and permitting consent to be coercively obtained. Make no mistake about it: despite the comforting tone of the bureaucratic language, under the HIPAA-spawned regulations it is the federal government that henceforth will determine what medical data exchanges are considered "appropriate," what exchanges are "authorized by law," what constitutes patient "consent," and what "security" policies will be deemed sufficient.

People familiar with HIPAA's encroachments find few words strong enough to impart the magnitude of the threat to personal privacy involved. *Forbes* editor-in-chief Steve Forbes described it as a "breathtaking assault on the sanctity of your medical records"; *Newsweek*'s writers described the "big, ugly fact" that under HIPAA "every detail of your medical profile may well land in this new system without your consent," explaining that the new national databank will allow "[a]nyone who knows your special health-care number" to be "privy to some of your most closely guarded secrets."[62]

Despite such outcries, even today neither the public nor the media have fully awakened to the scope of HIPAA. When the *New York Times* on July 20, 1998, ran a front-page story entitled "Health Identifier For All Americans Runs Into Hurdles," the nearly two-year-old fact that such a unique health identifier was mandated by statutory law was described elsewhere in the media as breaking news. Depicting the Clinton administration as "quietly laying plans to assign every American a 'unique health identifier,'" the *Times* described the identifier as a "computer code that could be used to create a national database that would track every citizen's medical history from cradle to grave."

Meanwhile the federal bureaucracy proceeded systematically to carry out its statutory duty to select a health identifier. Yet even as HHS was developing a "White Paper" suggesting alternative ways of implementing the identifier, the administration tried to soothe the public by falsely asserting a personal "confidentiality right," a "'right to communicate with health care providers in confidence and to have the confidentiality of the individually identifiable health care information protected,'" as proclaimed in November 1997 by the President's Quality Commission. Of course, no one knowledgeable of HIPAA's electronic database and health identifier provisions had objective grounds for believing such rights to be secure under existing statutory law. Indeed, HHS itself stated in 1998 that the President's Quality Commission and the HHS secretary already had "recognized that we must take care not to draw the boundaries of the health care system and permissible uses of the unique identifier too narrowly."[64] Given the predilections of federal officials and the proposals at hand, the problem is quite the opposite.

On July 2, 1998, HHS released its lengthy White Paper entitled "Unique Health Identifier for Individuals." In this chilling document HHS calmly discussed exactly

what Orwellian form the "unique health identifier" would take and what degree of encroachment on individual privacy would be compelled. Along with other proposals, HHS considered the following alternatives, suggested by the American National Standards Institute (ANSI), as "candidate identifiers":

- Social Security number (SSN), including the proposal of the Computer-based Personal Record Institute (CPRI);
- Biometric identifiers;
- Directory service;
- Personal immutable properties;
- Patient identification system based on existing medical record number and practitioner prefix;
- Public key-private key cryptography method; and a sample
- Universal Healthcare Identifier (UHID) developed by the American Society for Testing and Materials (ASTM).

In evaluating these and other proposals, HHS grouped them into four categories: those based on the SSN, those not based on the SSN, those that don't require a "universal, unique identifier," and hybrid proposals. Despite the range of alternatives, HHS noted that "Many of the proposals involve either the SSN, SSA's enumeration process [including its "Enumeration at Birth" process], or both."

The federal drive to link birth and death records with SSNs seen elsewhere also recurred here, in this case augmented by linkage to the health identifier. Noting that all SSN-dependent proposals would "benefit from further improvements in the process for issuing and maintaining both SSNs and birth certificates," the HHS document suggested that an "improved process could begin with a newborn patient in the birth hospital" where "at once the proper authorities would assign a birth certificate number, assign an SSN, and assign the health identifier."[65] That goal echoes throughout today's multifaceted federal data-collection efforts.

In considering SSN-based health identifiers, HHS listed as a positive aspect of the unenhanced SSN that it "is the current de facto identifier" and that people "are accustomed to using their SSN as an identifier" and "would not be required to adjust to change." One alternative proposal would add to the SSN a "check digit" for fraud control. Another would "use the SSN as the health identifier for those individuals to whom it is acceptable, but offer an alternative identifier to others." From a political transaction-cost manipulation perspective that proposal holds appeal, for it would give the appearance of individual control without the reality. (Does anyone think that there wouldn't be a data table linking the SSN and the "alternative" identifier?) Amazingly, listed among potential negative aspects of this proposal was the fact that a "potential stigma could be attached to the alternate identifier" since "a request for the identifier might be interpreted to mean that the individual has something to hide"! HHS also was troubled by this proposal because of the department's "anticipat[ion] that, given the choice, significant numbers of individuals would request the alternate identifier."

Equally stunning were proposals to require biometric identifiers as the unique health identifier. The HHS White Paper described biometric identifiers as "based on unique physical attributes, including fingerprints, retinal pattern analysis, iris scan, voice pattern identification, and DNA analysis." Listed negative aspects of this alternative were chiefly mechanical obstacles—the fact that there is now "no infrastructure" to support such identifiers, that the necessary "special equipment" would "add to the cost" of this alternative, and the like.[66][67] Cost and equipment issues thus were set against the benefit of "uniqueness" that this alternative would provide. Only the fact that biometric identifiers are already used in law enforcement and judicial proceedings prompted HHS to state that their usage in health care might make it "difficult to prevent linkages that would be punitive or would compromise patient privacy." No mention was made of

No mention was made of loss of liberty or threat of a police state, unless that was what was meant by "linkages that would be punitive."

Doesn't anyone wonder why the central government would like to keep track of information about our library cards and membership in civil organizations?

loss of liberty or threat of a police state, unless that was what was meant by "linkages that would be punitive."

In addition to biometric identifiers, another proposal in the group not based on SSNs was a "civil registration system." Such a system would "use records established in the current system of civil registration as the basis to assign a unique, unchanging 16-position randomly-generated (in base 10 or base 16) identifier for each individual." This identifier "would link the lifetime records of an individual's human services and medical records" and "track these and other encounters with the civil system," including "state birth files," visas, "SSA records and military identification," and "library card and membership in civil organizations, etc."[68] Doesn't anyone wonder why the central government would like to keep track of information about our library cards and membership in civil organizations? HHS noted that although such a system "meets the requirement of HIPAA for a standard, unique health identifier for each individual," it "would be likely to raise very strong privacy objections." Evidently, from HHS's perspective, the public's "strong privacy objections" are the only barrier to police state methods.

A hybrid proposal that elicited strong HHS support was called "Universal Healthcare Identifier/Social Security Administration" (UHID/SSA). The UHID is an identifier up to 29 characters long, including a 16-digit sequential number, some check digits, and an "encryption scheme identifier." HHS noted that the UHID/SSA proposal, by selecting the SSA as a "trusted authority" to maintain the system, "echoes the call for improvements to the birth certificate process to ensure reliable issuance of SSNs and UHIDs at birth." The SSA would issue the UHID with each new SSN, and those without SSNs "would be issued UHIDs as they generate their first encounter with the health system." Although the UHID would not appear on the Social Security card, the "SSA would maintain the database linking the SSN with the health identifier for its internal verification process, but other unauthorized users would be prohibited from linking the two numbers." In conjunction with the UHID/SSA proposal, HHS praised the SSA as an "experienced public program with a national identification system that includes most U.S. citizens and with the infrastructure necessary to issue and maintain the health care identifier." HHS stated that selecting the SSA "as the responsible authority for assigning the health care identifier builds on the present infrastructure for issuing SSNs" and would allow us to "restrict the identifier to health care uses that can be protected with legislation or regulation."[69]

There was more, including some less intrusive measures, but these excerpts convey the spirit of this shocking document. In late July 1998, after the *New York Times* story publicized the issue, executive branch officials took steps to distance themselves from the unique health identifier. It was a remarkable display, given that the statutory provisions—including the lack of privacy restrictions—were Clinton administration creations. Nonetheless, on July 31 Vice President Al Gore ceremoniously proclaimed a new White House commitment to a multifaceted "Electronic Bill of Rights," which included, among many other things, restrictions on dissemination of people's medical records. Bowing to public pressure, the vice president said that the administration would not proceed with the unique health identifier until Congress passed appropriate privacy legislation.[70]

Soon thereafter, in fall 1998, Congress specifically prohibited HHS from spending money on developing a unique health identifier for individuals, initiating a moratorium that has been renewed annually. Nevertheless, HIPAA's statutory mandate was not repealed. The relevant language remains unequivocal, stating that the "Secretary shall adopt standards providing for a standard unique health identifier for each individual . . . for use in the health care system" and "shall adopt security standards" and standards to enable electronic exchange of health information.[71]

With a final HHS medical privacy rule now in place, Congress is well positioned to permit a unique health identifier standard to

be promulgated. After all, few have noticed that the much ballyhooed "privacy" rule actually reduces our privacy, permitting widespread dissemination of our personal medical records without our consent (as described in Chapter 6). The dominant message issuing from government officials and the popular press has been: relax; we have a privacy rule; no more need to worry! In this political context, politicians who support the federal powers granted by HIPAA possess the perfect transaction-cost-manipulating rationale for proceeding with the unique identifiers, no matter what the eventual consequences regarding our medical privacy.

One thing is clear: unless the relevant HIPAA provision is repealed, sooner or later the new health identifiers will become a reality. Under HIPAA, it is the law. Moreover, even if HIPAA's unique health identifier provision were repealed, our omnipresent Social Security numbers would serve the same function. In light of the 1998 HHS White Paper, the real question is how intrusive the identifiers will be. Other key rules, including the HHS "Standards for Electronic Transactions" discussed in Chapter 6, already have been promulgated to implement the uniform electronic databases of personal medical information and widespread data exchanges envisioned by HIPAA. The databases are under construction.

Once this medical information is assembled, its likely uses and constituencies will multiply. As early as June 1997, *Newsweek* reported that "[o]rganizations clamoring for unfettered access to the databank include insurers, self-insured employers, health plans, drugstores, biotech companies and law-enforcement agencies." Moreover, as with the U.S. Census, pressure will materialize to expand the centralized information's scope. By 1997 the National Committee on Vital and Health Statistics already had "tentatively recommended that this mother lode of medical information be further augmented by specifics on living arrangements, schooling, gender and race."[72]

The issue is not just privacy; it is government power. Dr. Richard Sobel of Harvard Law School understood this clearly. Assessing the impact of the new national database and unique health identifiers, he stated: "What ID numbers do is centralize power, and in a time when knowledge is power, then centralized information is centralized power. I think people have a gut sense that this is not a good idea."[73] Whether that "gut sense" will find effective political voice is the troublesome question.

Tracking Your Child's Education: The "National Center for Education Statistics"

If centralized information is centralized power, the information now being collected about children's educational performance is especially disturbing. Today federal data collection, its scope expanded by the 1994 education acts, permeates our educational system. As with medical and employment information, here too individually identified information is being centralized in cross-linked electronic databases nationwide, and we are again being asked to trust that it will not be misused.

Recent experience in Fairfax County, Virginia, suggests what such legislation has spawned. In January 1997 the *Washington Post* reported several Fairfax County school board members "challeng[ed] a planned $11 million computer database that would let schools compile electronic profiles of students, including hundreds of pieces of information on their personal and academic backgrounds." The database would "be used to track students from pre-kindergarten through high school" and "could include information such as medical and dental histories, records of behavioral problems, family income and learning disabilities." Fairfax was "considering providing some of the data to a nationwide student information network run by the U.S. Department of Education," possibly making the database "compatible

If centralized information is centralized power, the information now being collected about children's educational performance is especially disturbing.

with a nationwide data-exchange program, organized by the Department of Education, that makes student information available to other schools, universities, government agencies and potential employers."[74]

That nationwide data-exchange network—orchestrated by the federal government and extended through the 1994 education acts—now is the lifeblood of centralized data collection about American students and preschoolers, creating vast and potentially ill-protected computerized records about children and families throughout America. The data-exchange pathways are (perhaps intentionally) complex, largely connected via the Office of Educational Research and Improvement within the U.S. Department of Education (DOE).

That office, administered by the assistant secretary for educational research and improvement, stands at the apex of the data-centralization hierarchy, broadly empowered to "collect, analyze, and disseminate data related to education" and charged with "monitoring the state of education" in America.[75] Included within the Office of Educational Research and Improvement are

- the National Center for Education Statistics;
- five national research institutes;[76]
- the Office of Reform Assistance and Dissemination;
- the National Educational Research Policy and Priorities Board; and
- "such other units as the Secretary [of Education] deems appropriate."[77]

Horizontal data linkages between subordinate units in this hierarchy are made explicit by a statutory requirement that the Office of Reform Assistance and Dissemination create an "electronic network" linking most education-related federal offices as well as "entities engaged in research, development, dissemination, and technical assistance" through grants, contracts, or cooperative agreements with DOE.

The federal education network is further required to be linked with and accessible to other users such as state and local education agencies, providing file transfer services and allowing DOE to disseminate, among other things, "data published by the National Center for Education Statistics," a directory of "education-related electronic networks and databases," and "such other information and resources" as DOE "considers useful and appropriate." Sixteen regional "educational resources information center clearinghouses" support the data dissemination, along with a National Library of Education intended to serve as a "one-stop information and referral service" for all education-related information produced by the federal government.[78] Through the School-to-Work Opportunities Act the Labor Department is required to act jointly with DOE to "collect and disseminate information" on topics that include "research and evaluation conducted concerning school-to-work activities" and "skill certificates, skill standards, and related assessment technologies."[79]

A spider web of data exchange is the planned outcome. But central to the entire process is the National Center for Education Statistics (the "National Center"). It is the federal entity most directly and extensively involved in receiving individually identifiable information about American children and their education.

The National Center has authority to "collect, analyze, and disseminate statistics and other information relating to education" in the United States and elsewhere.[80] It is authorized to collect data on such things as "student achievement," the "incidence, frequency, seriousness, and nature of violence affecting students," and, still more intrusively, "the social and economic status of children." The clear implication is that schools will be required to obtain information from children and their families on such topics. In addition, to carry out the National Assessment of Educational Progress (NAEP), the commissioner of education statistics is authorized to "collect and report data . . . at least once every two years, on students at ages

The National Center for Education Statistics is the federal entity most directly and extensively involved in receiving individually identifiable information about American children and their education.

9, 13, and 17 and in grades 4, 8, and 12 in public and private schools."[81] States participating in the NAEP testing process thus generate additional individually identified student information for the federal government.

Making education data from diverse sources dovetail at the national level is an explicit federal objective. The commissioner of education statistics is authorized to gather information from "States, local educational agencies, public and private schools, preschools, institutions of higher education, libraries, administrators, teachers, students, the general public," and anyone else the commissioner "may consider appropriate"—including other offices within DOE and "other Federal departments, agencies, and instrumentalities" (the IRS, SSA, and federal health care database authorities come to mind). To facilitate centralization of the data, the commissioner is empowered to establish "national cooperative education statistics systems" with the states to produce and maintain "comparable and uniform information and data on elementary and secondary education, postsecondary education, and libraries" throughout America.[82]

The scope of these databases is so large and their information so personal that even Congress understood the need to genuflect toward privacy and confidentiality. Indeed, the education statutes purport to protect individually identifiable information, directing the federal bureaucracy to "develop and enforce" standards to "protect the confidentiality of persons" in its data collection and publication process. Individually identifiable information is said to be restricted to use for statistical purposes only. In addition, the NAEP provisions prohibit the commissioner of education statistics from collecting data "not directly related to the appraisal of educational performance, achievement, and traditional demographic reporting variables," admonishing the commissioner to insure that "all personally identifiable information about students, their educational performance, and their families" will remain "confidential."[83]

Unfortunately, such provisions do not guarantee the security of personal information. Aside from the possibility of illicit breaches of confidentiality, specific statutory exceptions to confidentiality requirements threaten to undermine any such security. To begin with, information about institutions and organizations that receive federal grants or contracts is not protected.[84] Moreover, the National Center's records—"including information identifying individuals"—are made accessible to a bevy of federal officials and their designees, including the U.S. comptroller general, the director of the Congressional Budget Office, and the librarian of Congress, as well as the secretary of education, again with the boilerplate admonition that individually identifiable information is to be used only for statistical purposes.[85] Separate DOE privacy regulations also countenance myriad disclosures without the consent of the subject individuals, among them disclosures made for "routine uses" (one of the major loopholes in the 1974 federal Privacy Act discussed above) and those made either to another government agency "for a civil or criminal law enforcement activity" or to Congress.[86]

The Family Educational Rights and Privacy Act (FERPA) similarly fails to protect individuals effectively against disclosure of student information to the federal government. Although FERPA's rules in general prevent educational agencies and institutions from disclosing personal information about students without their consent, FERPA explicitly permits release of such information to authorized representatives of the U.S. comptroller general, the secretary of education, and state educational authorities whenever individually identifiable records are "necessary in connection with the audit and evaluation of Federally-supported education program[s], or in connection with the enforcement of the Federal legal requirements" related to such programs. In other words, FERPA simply does not protect us against disclosure of student records to the federal government. Again federal bureaucrats are admonished that, unless "collection of personally identifiable information is specifically authorized" by federal law, "any data collected by such officials shall be protected in a manner

Aside from the possibility of illicit breaches of confidentiality, specific statutory exceptions to confidentiality requirements threaten to undermine security.

which will not permit the personal identification of students and their parents by *other than those officials,* and such personally identifiable data shall be destroyed when no longer needed" for the above purposes.[87] How such destruction could be enforced and electronic copies prevented are unanswered—and unanswerable—questions. The officials themselves have unquestioned access to such personally identified information, without the subject individual's consent. That much lawmakers intended.

But disclosures beyond those intended by lawmakers also are inevitable. Together the statutes have spawned huge databases containing individually identifiable personal and educational information, widely distributed, whose use is supposed to be confined to "statistical" endeavors. The laws don't block the government's collection of individually identifiable information, only its use. The risk analogy cited earlier—giving a teenager keys to a motorcycle, handing him a bottle of liquor, and admonishing him not to drink and drive—is applicable; once again we're just "asking for trouble." Even criminal penalties authorized for individuals convicted of violating confidentiality provisions of these laws do little to lessen legitimate privacy concerns.

Disclosures beyond those intended by lawmakers also are inevitable.

By placing vast discretion regarding collection and distribution of personal information in the hands of federal officials, and by largely preventing citizens from blocking transfer of information to the central government, these laws again subordinate privacy to the imperative of federal prying into people's private lives. As Electronic Privacy Information Center director Marc Rotenberg remarked concerning compilation of databases on students such as those proposed in Fairfax County, "'The privacy concerns are really extraordinary.'"[88]

Tracking Your Bank Account: The Bank Secrecy Act and Its Progeny

Privacy in America is further jeopardized by federal statutory law requiring banks and other financial institutions to create permanent records of each individual's checks, deposits, and other banking activities. Along with the FDIC's ill-fated proposal[89] in December 1998 to require banks to scrutinize every customer's banking records for evidence of "unusual" transactions—which in effect would have mandated warrantless searches of private financial records—the legislation authorizing these intrusions and U.S. Supreme Court cases upholding them illuminate the tenuous status of privacy in America today.

The pivotal legislation was the Bank Secrecy Act of 1970.[90] In the name of assembling banking records with "a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings," Congress empowered the secretary of the treasury to require every federally insured bank to create:

> 1. a microfilm or other reproduction of each check, draft, or similar instrument drawn on it and presented to it for payment; and
> 2. a record of each check, draft, or similar instrument received by it for deposit or collection, together with an identification of the party for whose account it is to be deposited or collected.[91]

That requirement entailed microfilm records of every detail of each customer's bank account—each check, each deposit—with each account identified by the holder's Social Security number.[92] The statute authorized similar record keeping to be required of uninsured institutions, including even credit card companies.[93] Putting further discretionary power in the treasury secretary's hands, the simultaneously passed Currency and Foreign Transactions Reporting Act required individuals and financial institutions to report the "payment, receipt, or transfer of United States currency, or such other monetary instruments as the Secretary may specify, in such amounts, denominations, or both, or under such circumstances, as the Secretary shall by regulation prescribe."[94] What could

not be learned about an individual from such records?

Court challenges quickly arose. In 1974 the U.S. Supreme Court in *California Bankers Association v. Shultz* upheld the constitutionality of the record-keeping requirements of the Bank Secrecy Act against challenges grounded in the First, Fourth, and Fifth Amendments to the U.S. Constitution.[95] Although the Court stated that the act did not abridge any Fourth Amendment interest of the banks against unreasonable searches and seizures, the Court explicitly reserved the question of the Fourth Amendment rights of banks' customers if bank records were disclosed to the government as evidence through compulsory legal process. The Court stated that "[c]laims of depositors against the compulsion by lawful process of bank records involving the depositors' own transactions must wait until such process issues." Dissenting, Justice Thurgood Marshall stated:

> The plain fact of the matter is that the Act's recordkeeping requirement feeds into a system of widespread informal access to bank records by Government agencies and law enforcement personnel. If these customers' Fourth Amendment claims cannot be raised now, they cannot be raised at all, for once recorded, their checks will be readily accessible, without judicial process and without any showing of probable cause, to any of the several agencies that presently have informal access to bank records.[96]

Justice Marshall added that it was "ironic that although the majority deems the bank customers' Fourth Amendment claims premature, it also intimates that once the bank has made copies of a customer's checks, the customer no longer has standing to invoke his Fourth Amendment rights when a demand is made on the bank by the Government for the records." He called the majority's decision a "hollow charade" whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late.[97]

Justice Marshall's "hollow charade" assessment was vindicated two years later by the Court's 1976 decision in *United States v. Miller*.[98] Stating flatly that depositors have "no legitimate 'expectation of privacy'" in their bank records, the Court there held that the "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government," a conclusion not altered by the fact that the Bank Secrecy Act mandated creation of the records.[99] Accordingly, the Court held that a depositor's Fourth Amendment rights were not abridged by the government's acquisition of account records from his banks as part of a criminal prosecution, even if the subpoena for the documents was defective.

The case was too much for even Congress to stomach. In response to *U.S. v. Miller,* Congress in 1978 passed the Right to Financial Privacy Act ("Financial Privacy Act"), attempting to restore some protection of personal financial records in the wake of the Bank Secrecy Act's forced disclosures.[100] The central idea of the Financial Privacy Act was to prevent federal government authorities from obtaining personal financial records held by banking institutions unless either the customer authorized the disclosure or the bank was responding to a properly issued subpoena, administrative summons, search warrant, or "formal written request" by a government authority.[101]

In broad outline, the act prohibits banks from disclosing personal financial records maintained pursuant to the Bank Secrecy Act unless the federal authority seeking those records "certifies in writing to the financial institution that it has complied" with the Financial Privacy Act.[102] That certification may be based on any of the above rationales including a federal official's "formal written request," the lenient prerequisites for which potentially undermine the statute's core objectives. Such a request requires mere government assertion that "there is reason to believe that the records sought are relevant to

The case was too much for even Congress to stomach. In response to *U.S. v. Miller,* Congress in 1978 passed the Right to Financial Privacy Act.

We continue to rely on Congress—the very source of the initial privacy breach—to formulate laws supposed to protect our financial privacy.

a legitimate law enforcement inquiry," accompanied by government notification of the bank customer at his last known address.

But "law enforcement inquiry" is used as a term of art in the statute. Defining it to include any "official proceeding" inquiring into a failure to comply with a "criminal or civil statute or any regulation, rule, or order issued pursuant thereto," the statute explicitly includes the broad sweep of federal regulatory matters and thereby radically expands the bank records that can be targeted and disclosed in the name of "law enforcement inquiry." Moreover, the notification requirement can be met by simply mailing a copy of the request to the targeted bank customer "on or before the date on which the request was made to the financial institution." Unless the individual then takes specific steps to resist the disclosure by filing and substantiating a motion with a U.S. district court within fourteen days after the request was mailed (not received), the bank is permitted to give the government the records it wants. Once obtained by federal authorities, the bank records can be shared with other federal agencies or departments if the transferring entity certifies in writing that there is "reason to believe that the records are relevant to a legitimate law enforcement inquiry within the jurisdiction of the receiving agency or department."[103] In light of such procedural impediments to private resistance and the magic words "law enforcement activity" that allow countless channels of federal access to personal bank records, it is clear in whose favor the deck is stacked.

Besides the looseness evident in these statutory provisions, two other major problems pervade the Financial Privacy Act: its specific exclusions and, more generally, the unreliability of Congress as protector of financial privacy. Sixteen listed "exceptions" to the Financial Privacy Act allow government authorities to avoid its provisions in a wide variety of circumstances.[104] In addition, the act allows government authorities to obtain emergency access to financial records from banks and other financial institutions in certain situations.[105]

These exceptions along with the porosity of the statute's strictures made the Financial Privacy Act weak grounds for protection from unwarranted federal scrutiny of our personal bank transactions. Of course, that is no surprise. We surely cannot expect federal officials who still claim power to order third-party microfilming of our personal banking records to always show delicate restraint in using them. Yet we continue to rely on Congress—the very source of the initial privacy breach—to formulate laws supposed to protect our financial privacy.

It happened again in 1999 with passage of the Gramm-Leach-Bliley Act.[106] That act repealed the 1933 Glass-Steagall Act and loosened legal restrictions on banks' ability to engage in related endeavors such as securities transactions.[107] Old barriers between banking, insurance, and securities businesses were removed. A vast array of financial services thus could be provided by affiliated companies, creating enormous potential economic efficiencies.

Unfortunately, the Gramm-Leach-Bliley Act also created an enormous threat to the privacy of personal information held by the newly interlocked companies. To ease our minds, the authors of the act mandated certain privacy procedures for affected financial institutions, stating that it is "the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information."[108] Despite those fine words, however, the privacy regulations again were stacked against the actual preservation of privacy.

Consider first the pass-through of personal financial information to the government permitted by the Gramm-Leach-Bliley Act. After setting forth rules intended to limit financial firms' disclosure of personal information to nonaffiliated third parties, the act then listed numerous exceptions to those privacy rules, allowing extensive disclosure of personally identifiable information, among

them

- disclosures "to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury . . ., a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety"; and
- disclosures "to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law."[109]

In other words, having facilitated much broader integration of personal data by financial firms, Congress immediately made provision for the federal government and state governments to get their hands on it.

It is therefore not surprising that the Gramm-Leach-Bliley Act's restraints on financial firms also were structured to make sure that lots of personal data would be shared. The act requires financial institutions to notify customers periodically of the institution's disclosure and privacy policies regarding affiliated as well as nonaffiliated parties. With respect to nonaffiliated third parties, however, the main restraint on disclosure was structured as an "opt out" provision that requires a financial institution to send customers a notice (a) describing the disclosures of their personal information that the firm may make to nonaffiliated third parties, and (b) specifying to whom the customer should write to prevent such disclosure.[110] If the customer fails to communicate his objection to the disclosure, the disclosure can legally occur. That is why we have been receiving all those little "Our Privacy Policies" pamphlets with all that little tiny print. Among those who would prefer not to have personal information about themselves shared with nonaffiliated companies, how many do you suppose take the time to read and respond to each of those little pamphlets? And how many would consent if the pamphlets instead asked for our actual permission to disclose that personal information about us? Of course, Congress understands these realities as well as we do.

As obliging Congresses continue to cobble together loose statutes such as the Gramm-Leach-Bliley privacy provisions and the Financial Privacy Act, we now know that even such porous protections could be withdrawn, our financial privacy utterly destroyed, without constitutional objection from the U.S. Supreme Court. In such circumstances, congressional architects of the nationwide structure of financial records now threatening our privacy are unlikely to provide reliable protection.

Government As Privacy Protector?

In 1974 Congress passed the omnibus Privacy Act, cited earlier in this chapter, to regulate disclosure of personal information by federal agencies. Even that long ago Congress recognized the damage that federal record keeping and disclosure could do, as lawmakers made explicit in the "findings" accompanying the act:

1. the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;
2. the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
3. the opportunities for an individual

We now know that even porous protections could be withdrawn, our financial privacy utterly destroyed, without constitutional objection from the U.S. Supreme Court.

to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

4. the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
5. in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.[111]

Despite that clear acknowledgement of the federal threat to personal privacy, the 1974 Privacy Act[112]—riddled with exceptions and counterbalanced by disclosure mandates in the Freedom of Information Act —failed to fulfill the promise these declarations seemed to hold. The Electronic Frontier Foundation was unequivocal in its 1994 assessment, stating that in meritorious cases "it is extremely difficult for individuals to obtain relief under the . . . Privacy Act" and calling the Act's bias in favor of government record keepers "one of the most ugly faces of privacy."[113]

No stronger proof of the act's failure could be given than the fact that all of the privacy-destroying measures discussed in this chapter were initiated or sustained after the Privacy Act's adoption and are deemed compatible with its mandates. The federally required expansion of use of Social Security numbers, the federal databases of "new hires," the employment-authorization databases, the federal mandates for uniform electronic databases of personal health information and "unique health identifiers," the expanded federal collection of individually identified educational information, the continued federal requirement that financial institutions microfilm our checks and deposits in case the federal government desires to examine them—all of these now coexist with a law ostensibly assuring our privacy vis-à-vis federal government "collection, maintenance, use, and dissemination" of personal information.

In 1988, as people became increasingly alarmed about government centralization of personal information, Congress purportedly sought to strengthen the Privacy Act by adding the Computer Matching and Privacy Protection Act.[114] Again, however, the statutory privacy protections amounted to less than met the eye, creating procedural hurdles rather than firm obstacles to database matching. The 1988 act continued to allow such exchanges provided that the "computer matching program" was "pursuant to a written agreement between the source agency and the recipient agency" that met specified procedural requirements. Federal database-matching activities through the "new hires" database, pilot programs for work authorization, child support enforcement programs, and other programs confirm that this act provided scant impediment to the continuing federal data quest. As noted earlier, some forty-seven instances of federal database exchanges involving personal information about Americans occurred pursuant to this statute within a recent eighteen-month period alone. Based on this and other evidence, Privacilla.org concluded in its 2001 report that the Computer Matching and Privacy Protection Act, by "regularizing transfer of citizen data among federal agencies," in reality "sanctions and contributes to the federal government's threat to privacy."[115] Openly acknowledging such ongoing federal data-sharing activity—indeed bragging about it—a government report published in 1998 reassured citizens that their information-collection burden is minimized because "Agencies are working together to share information across programs so that people only need respond to a single collection from one agency rather than multiple collections from many agencies."[116]

Federally required databases of personal information continue to proliferate.

Today, federally required databases of personal information continue to proliferate. One measure of their current scope is that, in the 2000 *Code of Federal Regulations,* the *index entry* under the heading "Reporting and recordkeeping requirements" by itself was

sixty-four pages long! Moreover, the federal government now reports an annual "information collection budget" showing the number of hours acknowledged to be the central government's "information collection burdens imposed on the public." For fiscal year 2000 that document estimated 7,447,200,000 hours—over seven billion hours—as the time cost of the information collection burden imposed on private citizens by federal departments and agencies.[117] That is equivalent to forcing over three and a half million private individuals to work full time at uncompensated labor for the entire year just to gather the data that the federal government demands.

Information on such a scale would not be collected unless federal officials regarded it as instrumental in changing people's behavior—social behavior, economic behavior, political behavior. And, of course, it is: collective outcomes as well as actions by individuals can be and are influenced by means of such programs. Far from innocuous, this data collection and the intensity of its pursuit reveal the enormous value placed on such intelligence by federal officials. Rep. Jim McDermott (D., Wash.), one of the few congressmen who actively resisted HIPAA's 1996 authorization of uniform national electronic databases for health care, later stated, "There is no privacy anymore," adding that "It has been eroded in so many ways that you can find out almost anything about anybody if you know how to work the computer well enough."[118]

Others cite the fundamental inconsistency between privacy and government. Noting that "privacy is inconsistent with so much of what government does," a 2001 report prepared by Privacilla.org stated that "[e]ven the best-intended government programs have as part of their design the removal of citizens' power over information about themselves," often making it "outright illegal for citizens to protect their privacy." The report concluded that "[w]hen government has collected information from people under the authority of law, people's ability to protect privacy in that information is taken away."[119]

Legislation aside, the personal behavior of government officials offers little hope that they can be trusted to behave ethically with respect to the personal data now at their fingertips. Republicans and Democrats alike succumb to temptation when the stakes are perceived to be high enough. Republican President Richard Nixon in 1971 expressed his intention to select as IRS commissioner "a ruthless son of a bitch," who "will do what he's told," will make sure that "every income tax return I want to see I see," and "will go after our enemies and not go after our friends."[120] It was widely reported that Democratic President Bill Clinton, for similar reasons, apparently sanctioned the illegal transfer of more than nine hundred FBI files to the White House. And, ironically, federal agencies such as the IRS routinely have used privacy legislation to shield evidence of their own misdeeds.[121] Does anyone contemplating today's ubiquitous federal collection of personal data still imagine that political leaders cannot and will not abuse this system for their own ends? Each passing administration demonstrates anew Dr. Sobel's succinct observation that "centralized information is centralized power."[122]

The converse is also true: with today's technology, centralized power is centralized information. Substantive powers of government spawn correlative record-keeping powers; as federal power grows, so does related data collection. Personal freedom accordingly gives ever more ground to expanding government responsibility. Given these inevitable tendencies, Cato Institute policy analyst Solveig Singleton proposed a better way to protect privacy:

> The better model for preserving privacy rights and other freedoms in the U.S. is to restrict the growth of government power. As the federal government becomes more entangled in the business of health care, for example, it demands greater access to medical records. As tax rates grow higher and the tax code more complex, the Internal

For fiscal year 2000 the federal government estimated over seven billion hours as the time cost of the information collection burden imposed on private citizens by federal departments and agencies.

> Revenue Service claims more power to conduct intrusive audits and trace customer transactions. Only holding back the power of government across the board will safeguard privacy—and without any loss of Americans' freedom.[123]

Of course, the Founders tried to hold back the power of government through the U.S. Constitution. As author and critic H. L. Mencken explained:

> [Government] could do what it was specifically authorized to do, but nothing else. The Constitution was simply a record specifying its bounds. The fathers, taught by their own long debates, knew that efforts would be made, from time to time, to change the Constitution as they had framed it, so they made the process as difficult as possible, and hoped that they had prevented frequent resort to it. Unhappily, they did not foresee the possibility of making changes, not by formal act, but by mere political intimidation—not by recasting its terms, but by distorting its meaning. If they were alive today, they would be painfully aware of their oversight.[124]

The federal data-collection programs now themselves serve as instruments of political transaction-cost augmentation.

As we have seen, this avoidance of the formal amendment process has been an integral part of the political transaction-cost manipulation undergirding the twentieth-century expansion of federal authority and the corresponding erosion of individual liberty.

Though fiercely concerned about privacy, for decades Americans have allowed the juggernaut of federal data collection to roll on, unmindful of writer and editor A. J. Nock's insight that "whatever power you give the State to do things *for* you carries with it the equivalent power to do things *to* you."[125] Public passivity on this issue reflects the usual politico-economic forces, central among them high costs of resistance exacerbated by federal officials' manipulation of political transaction costs. As we have seen, in repeated instances privacy-jeopardizing provisions have been hidden in omnibus bills hundreds of pages long, making it difficult for lawmakers, let alone citizens, to see them and react before they become law. Misinformation has also helped, especially when uncritically repeated by the media—the appealing justifications, the ignored data-collection authority. In the case of HIPAA, despite outspoken efforts in 1996 by Representative McDermott and several other legislators to publicize the extraordinary threat to privacy contained in the provisions for uniform electronic databases and unique health identifiers, neither Congress nor the media spread the story. Although some didn't know, some definitely did. Yet, two years later, face-saving untruths or careless reporting further obscured the events of 1996. When the "unique health identifier" story was reported in 1998 as breaking news, the Associated Press, for instance, uncritically reiterated statements attributed to an unnamed "Republican congressional aide" claiming that "[m]embers of Congress did not recognize the privacy implications of what they had done until media reports about the issue came out this week."[126]

Thus instituted, the federal data-collection programs described in this chapter now themselves serve as instruments of political transaction-cost augmentation. Their effect in raising the cost to individuals of resisting intrusive government power is evident. How might an individual even resist federal information collection about himself? With data largely collected by third parties and transferred to the central government without the subject individual's consent, personal information is now collected whenever an individual touches the fabric of society in almost any way: getting a job, seeking medical care, attending school, maintaining a bank account. Will not fear of government misuse of such personal information inevitably mold a more compliant citizenry?

Many who prize liberty and privacy—so easily assuaged, so vulnerable to political transaction-cost manipulation—were, in late 1998,

cheerfully celebrating a spurious victory regarding the unique health identifier, apparently comforted by Vice President Al Gore's commitment to an "Electronic Privacy Act." But the vice president's own press release, though it noted a raft of new controls the administration wanted to place on private businesses' use of personal information, was nearly silent regarding *government* use of personal information, stating only an intention to "launch a 'privacy dialogue' with state and local governments" that would include "considering the appropriate balance between the privacy of personal information collected by governments, the right of individuals to access public records, and First Amendment values."[127] With existing statutes and regulations usurping personal privacy more aggressively with each passing day, it is much too late for a bureaucratic "privacy dialogue."

And the federal government keeps pushing. On July 28, 1999, a news story titled "U.S. Drawing Plan That Will Monitor Computer Systems" ran on the front page of the *New York Times*. The report revealed a federal government proposal to establish a computer monitoring system "overseen" by the FBI that, among other things, would scrutinize private e-mail communications between individuals not suspected of any wrongdoing. The ostensible rationale for monitoring such private communication was "anti-terrorism" and protection against "intruders" attacking government computers. Reporter John Markoff summarized the proposal as follows:

> [The draft plan] calls for a sophisticated software system to monitor activities on nonmilitary Government networks and a separate system to track networks used in crucial industries like banking, telecommunications and transportation. . . . As part of the plan, networks of thousands of software monitoring programs would constantly track computer activities looking for indications of computer network intrusions and other illegal acts. The plan calls for the creation of a Federal Intrusion Detection Network, or Fidnet, and specifies that the data it collects will be gathered at the National Infrastructure Protection Center, an interagency task force housed at the Federal Bureau of Investigation. . . . The plan focuses on monitoring data flowing over Government and national computer networks. That means the systems would potentially have access to computer-to-computer communications like electronic mail and other documents, computer programs and remote log-ins.[128]

Civil liberties groups expressed their strong opposition to the proposal, likening the plan "to a computerized version of a random search."[129] James Dempsey, a staff lawyer for the Center for Democracy and Technology, said that the plan "involves monitoring all legitimate communications in order to identify the few unauthorized communications . . . a potential civil-liberties nightmare."[130]

The invasive statutes and regulations described in this chapter have brought us to this point. The government data collection now authorized would have seemed unimaginable in an America whose citizens once boldly and meaningfully proclaimed individual liberty. What important personal information is not now at the fingertips of curious federal officials? Whatever does remain private is increasingly vulnerable to proposals such as the one just described. And the future? Centralized power is centralized information; centralized information is centralized power. The usual consequences are well known: "As history has shown, the collection of information can have a negative effect on the human ability to make free choices about personal and political self-governance. Totalitarian regimes have already demonstrated how individuals can be rendered helpless by uncertainty about official use of personal information."[131]

Reducing central government power is the only alternative to such dependence. As government data mandates proliferate and

It is much too late for a bureaucratic "privacy dialogue."

Reducing central government power is the only alternative to dependence.

encryption issues loom larger, those who cling to government as privacy's bulwark may well reflect on Electronic Frontier Foundation cofounder John Perry Barlow's statement that "[t]rusting the government with your privacy is like having a peeping Tom install your window blinds."[132] In assessing the privacy implications of the mandated unique health identifiers and uniform electronic databases of personal medical information, physician Bernadine Healy was succinct: "Government does a lot of things well, but keeping secrets is not one of them."[133]

Notes

This chapter is adapted and reprinted with permission of the publisher from my article, "Watching You: Systematic Federal Surveillance of Ordinary Americans," *Independent Review: A Journal of Political Economy,* vol. 4, no. 2, Fall 1999 pp. 165–200, © Copyright 1999, The Independent Institute, 100 Swan Way, Oakland, California 94621-1428; http://www.independent.org.

1. Harry B. Acton, *The Morals of Markets: An Ethical Exploration,* in David Gordon and Jeremy Shearmur, eds., *The Morals of Markets and Related Essays* (1971; reprint, Indianapolis: Liberty Fund, 1993), p. 133.

2. Paul Schwartz, "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer," *Hastings Law Journal,* vol. 43, 1992, part 2, pp. 1321–89, at pp. 1363–64.

3. Ibid., pp. 1343 ("powerful way to control"), 1374 ("mysterious, incalculable bureaucracy").

4. Government collection of trade data and business information is not discussed here. Those important aspects of government data collection were highlighted by the Environmental Protection Agency's expansion of its "Toxic Release Inventory" to require businesses to report production data so detailed that Kline & Co. (a member of the Society of Competitive Intelligence Professionals) judged its wartime impact as "the equivalent of having the U.S. voluntarily turn over its code book to its enemies." Quoted in Pranay Gupte and Bonner R. Cohen, "Carol Browner, Master of Mission Creep," *Forbes,* October 20, 1997, pp. 170–77, at p. 176. Posting the information on its Internet website, the EPA "overrode heated industry protests and made it easy for corporate trade secret thieves to make off with billions of dollars' worth of America's most proprietary trade secrets." James A. Srodes, "Protect Us from Environmental Protection," *World Trade,* July 1998, pp. 14–15, at p. 14. See also 15 U.S.C. secs. 4901-11 (1998); 15 U.S.C. secs. 175–76, 178, 182 (1997).

5. Claire Wolfe, "Land-Mine Legislation," 1997. Posted by America-Collins, http://www.america-collins.com (Internet); america-collins@america-collins.com (E-mail); 5736 Highway 42 North, Forsyth, Georgia 31029, 912-994-4064 (office).

6. Simon G. Davies, "Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine," *Information Technology & People,* vol. 7, no. 4, 1994.

7. Ibid. ("Nazi Germany").

8. Solveig Singleton, "Don't Sacrifice Freedom for 'Privacy,'" *Wall Street Journal,* June 24, 1998, p. A18 ("Japanese-Americans"). See also Solveig Singleton, "Privacy As Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," Policy Analysis no. 295 (Washington, D.C.: Cato Institute, 1998).

9. The long form of the 1990 U.S. Census required respondents to answer questions about their ancestry, living conditions (including bathroom, kitchen, and bedroom facilities), rent or mortgage payment, household expenses, roommates and their characteristics, in-home telephone service, automobile ownership, household heating and sewage systems, number of stillbirths, language capability, and what time each person in the household usually left home to go to work during the previous week. The form stated that "By law [Title 13, U.S. Code], you're required to answer the census questions to the best of your knowledge," adding that the information requested "enable[s] government, business, and industry to plan more effectively." Nowhere did it state that sec. 221, Title 13 of the U.S. Code also specifies a maximum penalty of $100 for someone who chooses not to answer. See U.S. Dept. of Commerce, Bureau of the Census, 1990, Form D-2 (OMB no. 0607-0628). Except for the stillbirth and in-home telephone service inquiries, all of the above questions were repeated in the 2000 U.S. Census long form. U.S. Dept. of Commerce, Bureau of the Census, 2000, Form D-61B (OMB no. 0607-0856).

10. Simon G. Davies, "Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine" ("vague memory").

11. Ibid.

12. Schwartz, "Data Processing and Government Administration: The Failure of the American Legal

Response to the Computer," p. 1356, n. 165 (describing each individual's social security number as a "de facto national identification number").

13. Department of Health and Human Services, *Unique Health Identifier for Individuals: A White Paper* (Washington, D.C.: July 2, 1998), sec. III(A)(1).

14. Kristin Davis, quoted in Theodore J. Miller, "Look Who's Got Your Numbers," *Kiplinger's Personal Finance,* July 1998, p. 8. Kristin Davis authored "The Bonnie and Clyde of Credit Card Fraud" in the same *Kiplinger's* issue at pp. 65–71. Theodore Miller is the magazine's editor.

15. President Franklin D. Roosevelt, "Numbering System for Federal Accounts Relating to Individual Persons," Executive Order 9397, November 22, 1943. Reproduced in *Code of Federal Regulations,* Title 3 (Washington, D.C.: U.S. Government Printing Office, 1957), chapter 2, pp. 283–84.

16. William H. Minor, "Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections," *Columbia Journal of Law and Social Problems,* vol. 28, no. 2, 1995, pp. 253–96, at pp. 262–63. See also Robert Pear, "Not for Identification Purposes (Just Kidding)," *New York Times,* July 26, 1998, the *New York Times* on the Web. Some people seemed reluctant to admit what was being done with SSNs. When I wrote to complain about usage of my SSN as my "account number" on my federally insured student loan, a "loan servicing representative" from Academic Financial Services Association (AFSA) replied: "Your AFSA account number is not your social security number since it begins with a portfolio number SM 799 B followed by 10 digits"--despite the fact that my Social Security number constituted the next nine of those digits. I see his point: it's really so much different if "SM 799 B" precedes one's Social Security number! (Letter of June 11, 1986).

17. *Privacy Act of 1974,* Public Law 93-579, 93d Cong., 2d sess., December 31, 1974, 88 Stat. 1896. Codified to 5 U.S. Code sec. 552a (1996).

18. *Tax Reform Act of 1976,* Public Law 94-455, 94th Cong., 2d sess., October 4, 1976, 90 Stat 1525 ff., at 90 Stat. 1711-12. This law also made mandatory use of the SSN for federal tax purposes a matter of statutory law rather than IRS regulation. See William H. Minor, "Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections," *Columbia Journal of Law and Social Problems,* vol. 28, no. 2, 1995, pp. 253–96, at pp. 264–65 on this point.

19. See Department of Health and Human Services, *Unique Health Identifier for Individuals: A White Paper,* sec. III(A)(3).

20. See, for example, Public Law 105-34, 105th Cong., 1st sess., August 5, 1997, Title X, secs. 1090(a)(2), (4), 111 Stat. 961–62, which amended the statute governing the Federal Parent Locator Service to provide that "Beginning not later than October 1, 1999, the information referred to in paragraph (1) [42 U.S.C. sec. 653(b)(1), governing "Disclosure of information to authorized persons"] shall include the names and social security numbers of the children of such individuals" and further that the "Secretary of the Treasury shall have access to the information described in paragraph (2) [42 U.S.C. sec. 653(b)(2)] for the purpose of administering those sections of Title 26 which grant tax benefits based on support or residence of children." See also 42 U.S.C. secs. 651–52 for relevant AFDC provisions.

21. *Omnibus Consolidated Appropriations Act, 1997,* Public Law 104-208, 104th Cong., 2d sess., September 30, 1996, 110 Stat. 3009; *Illegal Immigration Reform and Immigrant Responsibility Act of 1996,* Public Law 104-208, 104th Cong., 2d sess., Division C, September 30, 1996, 110 Stat. 3009-546 ff.

22. Department of Transportation, National Highway Traffic Safety Administration, Proposed Rule, "State-Issued Driver's Licenses and Comparable Identification Documents," *Federal Register,* vol. 63, June 17, 1998, pp. 33219–25; *Code of Federal Regulations,* Title 23, Part 1331. In a passage that would make the Framers' blood boil, the Department of Transportation explained that, under the proposed rule, "States must demonstrate compliance with the requirements of the regulation by submitting a certification to the National Highway Traffic Safety Administration."

23. *Department of Transportation and Related Agencies Appropriations Act,* 2000, Public Law 106-69, 106th Cong., 1st sess., October 9, 1999, 113 Stat. 986, sec. 355, at 113 Stat. 1027.

24. *Illegal Immigration Reform and Immigrant Responsibility Act of 1996,* Public Law 104-208, 110 Stat. 3009-716, sec. 656(a).

25. Ibid., sec. 657. Virtually identical language was included in the *Personal Responsibility and Work Opportunity Reconciliation Act of 1996,* Public Law 104-193, 104th Cong., 2d sess., August 22, 1996, 110 Stat. 2105, sec. 111.

26. Miller and Moore reported in 1995 that Drexler Technology Corporation recently had patented an "optically readable ID card . . . [that] can hold a picture ID and 1,600 pages of text," cards that could be mass produced for less than $5.00 each. John J. Miller and Stephen Moore, "A

National ID System: Big Brother's Solution to Illegal Immigration," Cato Policy Analysis no. 237 (Washington, D.C.: Cato Institute, September 7, 1995). Available at http://www.cato.org.

27. *Illegal Immigration Reform and Immigrant Responsibility Act of 1996,* Public Law 104-208, 110 Stat. 3009-719-20, sec. 657.

28. For example, see H.R. 231, 105th Cong., 1st sess., January 7, 1997, a proposed bill "To improve the integrity of the Social Security card and to provide for criminal penalties for fraud and related activity involving work authorization documents for purposes of the Immigration and Nationality Act." Section 1(c) of the bill stated: "NOT A NATIONAL IDENTIFICATION CARD—Cards issued pursuant to this section shall not be required to be carried upon one's person, and nothing in this section shall be construed as authorizing the establishment of a national identification card."

29. Privacilla.org, "Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information Is Systematic and Routine," Special Report, March 2001, p. 1 (available at http://www.privacilla.org).

30. Ibid.

31. Ibid., p. 3. Privacilla.org stated that "In fact, the list of programs *not* subject to the Computer Matching and Privacy Protection Act is longer than the list of programs that are." Emphasis in original.

32. *Code of Federal Regulations,* Title 20, Chap. III, Subpart C, sec. 401.120, April 1, 1997.

33. Ibid., sec. 401.25.

34. Schwartz, "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer," p. 1357.

35. Ibid., p. 1367.

36. Ibid., pp. 1367-69. Schwartz cites Jerrold Brockmyre, director, Michigan Office of Child Support Enforcement, as quoted in Nancy Herndon, "Garnish: Dad," *Christian Science Monitor,* November 28, 1988, at 25.

37. Ibid., p. 1369.

38. *Social Security Number Confidentiality Act of 2000,* Public Law 106–433, 106th Cong., 2d sess., November 6, 2000, 114 Stat. 1910 (H.R. 3218).

39. Stephen Moore, "A National Identification System," testimony before the House Judiciary Committee, Subcommittee on Immigration and Claims, May 13, 1997. Available at http://www.cato.org/testimony/ct-sm051397.html. Stephen Moore is an economist with the Cato Institute.

40. *Job Training Partnership Act,* Public Law 97-300, 97th Cong., 2d sess., October 13, 1982, 96 Stat. 1322; Public Law 102-367, 102d Cong., 2d sess., September 7, 1992, 106 Stat. 1085, sec. 405(a).

41. *Personal Responsibility and Work Opportunity Reconciliation Act of 1996,* Public Law 104-193.

42. Although it contains information about all working individuals, the National Directory of New Hires is housed within the federal government's "Federal Parent Locator Service."

43. Robert Pear, "Government to Use Vast Database to Track Deadbeat Parents," *New York Times,* September 22, 1997, the *New York Times* on the Web.

44. *Personal Responsibility and Work Opportunity Reconciliation Act of 1996,* Public Law 104-193, sec. 313(b).

45. Brigid McMenamin, "Payroll Paternalism," *Forbes,* April 16, 2001, p. 114.

46. *Personal Responsibility and Work Opportunity Reconciliation Act of 1996,* Public Law 104-193, sec. 311.

47. Ibid., sec. 311, sec. 316, sec. 317.

48. Miller and Moore, "A National ID System: Big Brother's Solution to Illegal Immigration."

49. *Illegal Immigration Reform and Immigrant Responsibility Act,* Public Law 104-208, sec. 403.

50. The basic program required the attorney general to secure participation by at least "5 of the 7 States with the highest estimated population of aliens who are not lawfully present in the United States." Ibid., sec. 401, 110 Stat. 3009-655 ff.

51. Ibid., sec. 403(a), 110 Stat. 3009-659 ff.

52. Ibid., 110 Stat. 3009-662, referencing *U.S. Code,* Title 8, sec. 1324a(a)(1)(A). See also *U.S. Code,* Title 8, sec. 1324a(e)(4).

53. Ibid., sec. 403(b), 110 Stat. 3009-662 ff. See also the discussion in the preceding section of this chapter of the now repealed sec. 656(b), 110 Stat. 3009-718 ("state-issued drivers licenses and comparable identification documents").

54. Ibid., sec. 403(c), 110 Stat. 3009-663 ff. At the same time, the Immigration and Naturalization Service (INS) has moved toward a "machine read-

able passport program" for aliens. A federal statute signed into law October 30, 2000, advanced a planned automated entry-exit control system for aliens by making airlines' and other carriers' electronic transmission of passenger data to the INS a prerequisite for visa waivers for aliens traveling on those carriers. See *Visa Waiver Permanent Program Act,* Public Law 106-396, 106th Cong., 2d sess., October 30, 2000, 114 Stat. 1637 ff. (H.R. 3767). Since U.S. citizens' passports already are machine readable, such automated passenger data collection systems hold the potential for U.S. government tracking of U.S. citizens traveling abroad.

55. Ibid., sec. 404(h), 110 Stat. 3009-665.

56. "Cathy" is created by nationally syndicated cartoonist Cathy Guisewite.

57. Moore, "A National Identification System," testimony May 13, 1997.

58. *Workforce Investment Act of 1998,* Public Law 105-220, 105th Cong., 2d sess., August 7, 1998, 112 Stat. 936 ff., sec. 309, 112 Stat. 1082–83.

59. McMenamin, "Payroll Paternalism," p. 120.

60. Moore, "A National Identification System," testimony May 13, 1997. He added: "I have worked in Washington for fifteen years mainly covering the federal budget, and I have never encountered a government program that didn't work—no matter how overwhelming the evidence to the contrary."

61. Department of Health and Human Services, National Committee on Vital and Health Statistics, *Toward a National Health Information Infrastructure* (Washington, D.C.: June 2000), sec. 5 (available at http://ncvhs.hhs.gov/NHII2kReport.htm). Quoted in *Health Freedom Watch* (March–April 2001), p. 5 (http://www.forhealthfreedom.org).

62. Steve Forbes, "Malpractice Bill," *Forbes,* October 6, 1997, p. 27. Ellyn E. Spragins and Mary Hager, "Naked before the World: Will Your Medical Secrets Be Safe in a New National Databank?" *Newsweek,* June 30, 1997, p. 84. Although the federal government already has access to millions of medical records through Medicare, Medicaid, and federal subsidies for State Children's Health Insurance Programs, the uniform electronic databases of health information authorized by HIPAA involve the government in everyone's health care, whether or not they receive federal subsidies. On the failure of the December 28, 2000, HHS final privacy regulations to safeguard this information, see Chapter 6.

63. Sheryl Gay Stolberg, "Health Identifier for All Americans Runs into Hurdles," *New York Times,* July 20, 1998, p. A1.

64. Department of Health and Human Services, *Unique Health Identifier for Individuals: A White Paper,* secs. II(B) ["confidentiality right," quoting the President's Quality Commission], II(C) ["not to draw the boundaries . . . too narrowly"].

65. Ibid., sec. III(A).

66. Ibid., secs. III(B)(1)-III(B)(3).

67. Ibid., sec. III(C)(2).

68. Ibid., sec. III(C)(4).

69. Ibid., sec. III(E)(1).

70. White House Press Release, "Vice President Gore Announces New Steps toward an Electronic Bill of Rights," July 31, 1998. See also John Simons, "Gore to Propose Consumer-Privacy Initiative," *Wall Street Journal,* July 31, 1998, p. A12; Sheryl Gay Stolberg, "Privacy Concerns Delay Medical ID's," *New York Times,* August 1, 1998, the *New York Times* on the Web; Joel Brinkley, "Gore Outlines Privacy Measures, But Their Impact Is Small," *New York Times,* August 1, 1998, the *New York Times* on the Web.

71. For example, an HHS appropriations bill signed into law in December 2000 contained a section that stated: "None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C. 1320d-2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard." *Consolidated Appropriations Act,* 2001, Public Law 106-554, 106th Cong., 2d sess., December 21, 2000, 114 Stat. 2763, sec. 514 at 114 Stat. 2763A-71. *Health Insurance Portability and Accountability Act,* Public Law 104-191, 104th Cong., 2d sess., August 21, 1996, 110 Stat. 1936, sec. 262(a), amending 42 U.S.C. 1301 et seq. by adding sec. 1173.

72. Spragins and Hager, "Naked before the World," p. 84.

73. Dr. Richard Sobel, Harvard Law School, quoted in Sheryl Gay Stolberg, "Health Identifier for All Americans Runs into Hurdles," p. A13.

74. Tod Robberson, "Plan for Student Database Sparks Fears in Fairfax," *Washington Post,* January 9, 1997, p. A01 (www.washingtonpost. com).

75. *Educational Research, Development, Dissemination,*

and Improvement Act of 1994, Public Law 103-227, 103d Cong., 2d sess., Title IX, March 31, 1994, 108 Stat. 212 ff., sec. 912.

76. These include the National Institute on Student Achievement, Curriculum, and Assessment; the National Institute on the Education of At-Risk Students; the National Institute on Educational Governance, Finance, Policy-Making, and Management; the National Institute on Early Childhood Development and Education; and the National Institute on Postsecondary Education, Libraries, and Lifelong Education. See ibid., sec. 931.

77. Ibid., Public Law 103-227, sec. 912.

78. Ibid., sec. 941(f) (clearinghouses); sec. 951(d) (national library of education). The statute also amended federal vocational education legislation to require state boards of higher education to provide data on graduation rates, job placement rates, licensing rates, and high school graduate equivalency diploma (GED) awards to be "integrated into the occupational information system" developed under federal law. Ibid., sec. 991.

79. *School-to-Work Opportunities Act of 1994,* Public Law 103-239, 103d Cong., 2d sess., May 4, 1994, 108 Stat. 568 ff., sec. 404.

80. The functions of the National Center for Education Statistics were amended by the *Improving America's Schools Act,* Public Law 103-382, 103d Cong., 2d sess., October 20, 1994, 108 Stat. 4029 ff., Title IV, secs. 401 ff., at sec. 403. Title IV of the Improving America's Schools Act was entitled the National Education Statistics Act.

81. *National Education Statistics Act of 1994,* Public Law 103-382, 103d Cong., 2d sess., Title IV, October 20, 1994, 108 Stat. 4029 ff., sec. 404 ("violence"), sec. 411 ("grades 4, 8, and 12").

82. Ibid., sec. 405 ("may consider appropriate"), sec. 410 ("uniform information").

83. Ibid., sec. 411.

84. Ibid., sec. 408.

85 Ibid., sec. 408(b)(7).

86. *Code of Federal Regulations,* Title 34, Subtitle A, July 1, 1997, sec. 5b.9.

87. *Family Educational Rights and Privacy Act,* Public Law 93-380, 93d Cong., 2d sess., Title V, August 21, 1974, 88 Stat. 571, as amended, sec. 513. Emphasis added. Codified as *U.S. Code,* Title 20, sec. 1232g, 1998. See 20 U.S.C. sec. 1232g(b)(3) and sec. 1232g(b)(1)(C).

88. Quoted in Robberson, "Plan for Student Database Sparks Fears in Fairfax," p. A01.

89. Federal Deposit Insurance Corporation, Notice of Proposed Rulemaking, "Minimum Security Devices and Procedures and Bank Secrecy Act Compliance," *Federal Register,* vol. 63, December 7, 1998, pp. 67529–36. Withdrawal of the "Know Your Customer" proposal was announced in Federal Deposit Insurance Corporation, Withdrawal of Notice of Proposed Rulemaking, "Minimum Security Devices and Procedures and Bank Secrecy Act Compliance," *Federal Register,* vol. 64, March 29, 1999, p. 14845. The FDIC received 254,394 comments on the proposed mandate for "Know Your Customer" programs, of which only 105 favored the proposed rule.

90. Bank Secrecy Act of 1970, Public Law 91-508, 91st Cong., 2d sess., Title I, October 26, 1970, 84 Stat. 1114.

91. Ibid., sec. 101.

92. Although the Bank Secrecy Act's power extended to microfilming all checks and deposits, early on the secretary of the treasury decided to mandate microfilming of checks and deposits of $100 or more.

93. Public Law 91-508, Title I, sec. 123.

94 The Currency and Foreign Transactions Reporting Act comprised Title II of the same statute: *Currency and Foreign Transactions Reporting Act,* Public Law 91-508, 91st Cong., 2d sess., Title II, October 26, 1970, 84 Stat. 1118; see sec. 221, sec. 222. The act also required detailed reporting regarding monetary instruments of $5,000 or more received from or sent to individuals in places outside the United States. Regarding the federal government's exuberance in applying forfeiture penalties under this statute and a 1998 U.S. Supreme Court decision disallowing one exercise of such power, see Roger Pilon, "High Court Reins in Overweening Government," *Wall Street Journal,* June 23, 1998, p. A20; and James Bovard, "The Dangerous Expansion of Forfeiture Laws," *Wall Street Journal,* December 29, 1997, p. A11. The U.S. Supreme Court decision discussed in Pilon's article was *United States v. Bajakajian,* 524 U.S. 321 (1998).

95. *California Bankers Association v. Shultz,* 416 U.S. 21 (1974).

96. Ibid., 416 U.S. 51-52 ("must wait"); 416 U.S. 96-97 (Marshall dissenting).

97. Ibid., 416 U.S. 97.

98. *United States v. Miller,* 425 U.S. 435 (1976).

99. Ibid., 425 U.S. 442-43.

100. *Right to Financial Privacy Act,* Public Law 95-630, 95th Cong., 2d sess., Title XI, November 10, 1978, 92 Stat. 3697 ff.; codified to *U.S. Code,* Title 12, sec. 3401 ff.

101. Ibid., sec. 3402.

102 . The act also permits financial institutions to notify government authorities of information "which may be relevant to a possible violation of any statute or regulation," but such information is confined to identifying information concerning the account and the "nature of any suspected illegal activity." Ibid., sec. 3403.

103. Ibid., sec. 3401 ("law enforcement inquiry"), sec. 3408 (notification by mail), sec. 3412 (sharing records with other agencies).

104. Ibid., sec. 3413. These include, among other things, disclosure to the IRS pursuant to the Internal Revenue Code; disclosure pursuant to "legitimate law enforcement inquiry respecting name, address, account number, and type of account of particular customers"; disclosure pursuant to "Federal statute or rule promulgated thereunder"; disclosures pursuant to "consideration or administration" of Government loans or loan guarantees; disclosure sought to implement withholding taxes on Federal Old-Age, Survivors, and Disability Insurance Benefits; and disclosure to the Federal Housing Finance Board or Federal home loan banks. Moreover, in 1997 a district court held that the Financial Privacy Act does not apply to state or local government attempts to access these records. See *U.S. v. Zimmerman,* 957 F.Supp. 94 (N.D. W.Va., 1997).

105. Government authorities may obtain such emergency access if they declare that "delay in obtaining access to such records would create imminent danger of—(A) physical injury to any person; (B) serious property damage; or (C) flight to avoid prosecution," provided that they subsequently file in court a sworn statement by a supervisory official and provide notification as specified in the act. *Right to Financial Privacy Act,* Public Law 95-630, sec. 3414(b).

106. *Gramm-Leach-Bliley Act,* Public Law 106-102, 106th Cong., 1st sess., November 12, 1999, 113 Stat. 1338 (S. 900).

107. The Gramm-Leach-Bliley Act allowed financial holding companies to "engage in any activity" and to "acquire and retain the shares of any company engaged in any activity" that the regulators determine to be "financial in nature or incidental to such financial activity," or "complementary to a financial activity" so long as it "does not pose substantial risk to the safety or soundness of depository institutions or the financial system generally." Ibid., sec. 103(a). The law specifically stated that "[l]ending, exchanging, transferring, investing for others, or safeguarding money or securities" and "[p]roviding financial, investment, or economic advisory services, including advising an investment company" were to be considered as activities "financial in nature." "Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, and acting as a principal, agent, or broker for purposes of the foregoing" also were designated as permitted activities of financial holding companies. Ibid.

108. Ibid., sec. 501(a).

109. Ibid., sec. 502(e).

110. Ibid., sec. 502(b).

111. *Privacy Act of 1974,* Public Law 93-579, 93d Cong., 2d sess., December 31, 1974, 88 Stat. 1897, sec. 2(a). Codified to *U.S. Code,* Title 5, sec. 552a (1998).

112. *Freedom of Information Act,* Public Law 89-554, 89th Cong., 2d sess., September 6, 1966, 80 Stat. 383, as amended. Codified to *U.S. Code,* Title 5, sec. 552 (1998).

113. Quoted in Judith Beth Prowda, "Privacy and Security of Data," *Fordham Law Review,* vol. 64, 1995, pp. 738–69, at pp. 749–50.

114. *Computer Matching and Privacy Protection Act,* Public Law 100-503, 100th Cong., 2d sess., October 18, 1988, 102 Stat. 2507–14, sec. 2; codified at *U.S. Code,* Title 5, sec. 552a(o).

115. Privacilla.org, "Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information Is Systematic and Routine," Special Report, March 2001, p. 1 (47 database exchanges), p. 4 ("regularizing transfer"). Available at http://www.privacilla.org.

116. Office of Management and Budget, Office of Information and Regulatory Affairs, *Information Collection Budget of the United States Government--Fiscal Year 1999* (Washington, D.C.: U.S. Government Printing Office, 1999), p. 10.

117. Office of Management and Budget, Office of Information and Regulatory Affairs, *Information Collection Budget of the United States Government--Fiscal*

Year 2000 (Washington, D.C.: U.S. Government Printing Office, 2000), p. 83.

118. Quoted in Stolberg, "Health Identifier for All Americans Runs into Hurdles," p. A13.

119. Privacilla.org, "Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information Is Systematic and Routine," pp. 4–5.

120. Quoted by Wall Street Journal Board of Editors, "Politics and the IRS," *Wall Street Journal,* January 9, 1997, p. A10.

121. Shelley L. Davis, *Unbridled Power: Inside the Secret Culture of the IRS* (New York: HarperCollins, 1997), pp. 164–68.

122. As quoted above in Stolberg, "Health Identifier for All Americans Runs into Hurdles," p. A13.

123. Solveig Singleton, "Don't Sacrifice Freedom for 'Privacy,'" *Wall Street Journal,* June 24, 1998, p. A18.

124. H. L. Mencken, "The Suicide of Democracy," in Mayo DuBasky, ed., *The Gist of Mencken: Quotations from America's Critic* (May 12, 1940, *Baltimore Sun*; reprint, Metuchen, N.J.: Scarecrow Press, 1990), p. 350.

125. Albert Jay Nock, "The Criminality of the State," in Charles H. Hamilton, ed., *The State of the Union: Essays in Social Criticism* (Indianapolis: Liberty Fund, 1991), p. 274. Emphasis in original.

126. Associated Press, "Congress Won't Delay Medical Identification Law," posted by Cable News Network, July 23, 1998 (www.CNN.com).

127. White House Press Release, "Vice President Gore Announces New Steps Toward An Electronic Bill of Rights," July 31, 1998.

128. John Markoff, "U.S. Drawing Plan That Will Monitor Computer Systems," *New York Times,* July 28, 1999, p. A1, A16.

129. John Simons, "White House Computer-Monitoring Plan Raises Concerns over Civil Liberties," *Wall Street Journal,* July 29, 1999, p. A4.

130. Ibid., quoting James Dempsey. For an electronic copy of the government's draft plan ("National Plan for Information Systems Protection," dated June 7, 1999) see the Center for Democracy and Technology's website, http:// www.cdt.org/policy/terrorism/fidnet.

131. Paul M. Schwartz, "The Protection of Privacy in Health Care Reform," *Vanderbilt Law Review,* vol. 48, no. 2, 1995, pp. 295–347, at p. 307.

132. John Perry Barlow, quoted in Judith Beth Prowda, "Privacy and Security of Data," F*ordham Law Review,* vol. 64, 1995, pp. 738–69, at p. 765. Prowda cited Jeff Rose, "Right to E-mail Privacy Would Seem Self-Evident, *San Diego Union Tribune,* March 1, 1994 (Computerlink), at 3, as the source for the Barlow quotation.

133. Bernadine Healy, "Hippocrates vs. Big Brother," *New York Times,* July 24, 1998, p. A21.

Published by the Cato Institute, Cato Briefing Papers is a regular series evaluating government policies and offering proposals for reform. Nothing in Cato Briefing Papers should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Additional copies of Cato Briefing Papers are $2.00 each ($1.00 in bulk). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Avenue, N.W., Washington, D.C. 20001, call (202) 842-0200 or fax (202) 842-3490. Contact the Cato Institute for reprint permission.