
Watching You

Systematic Federal Surveillance of Ordinary Americans

— ◆ —

CHARLOTTE TWIGHT

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 payment, 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 just listed. 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, through magnetic strips and embedded computer chips capable of holding up to sixteen hundred pages of information about the individual. If a contemporary novelist were to

Charlotte Twight is a professor of economics at Boise State University.

The Independent Review, v.IV, n.2, Fall 1999, ISSN 1086-1653, Copyright © 1999, pp. 165–200

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 model for the foregoing description is a government that now wields exactly those awesome powers over the citizenry—America's federal government in 1999. In this article I substantiate each of the preceding statements and provide citations to the laws, regulations, and working papers establishing and designing such intelligence systems. The logical outgrowth of such all-encompassing federal collection of personal information has increased government power and concomitant individual dependence on government.

Governments have long recognized the capacity of information collection to erode individual autonomy by fostering deep personal uncertainty about the uses to which the information might be put. Paul Schwartz (1992) has described the 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. (1363–64)

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 mysterious, incalculable bureaucracy will be more likely to act as the government wishes them to behave. (1374)

With extensive federal data collection creating ever greater incentives to behave as government wishes us to behave, the societal result is metastasizing government control. Indeed, Schwartz views the computer's ability to digitize personal information as offering "the state and society a powerful way to control the behavior of individuals"

1. Government collection of trade data and business information is not discussed here. Those important aspects of government data collection were highlighted recently by the Environmental Protection Agency's expansion of its "Toxic Release Inventory" to require businesses to report production data so detailed that Kline and Co. (a member of the Society of Competitive Intelligence Professionals) judged its impact as "the equivalent of having the U.S. voluntarily turn over its code book to its enemies" in wartime (quoted in Gupte and Cohen 1997, 176). Posting the information on its Internet Web site, 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" (Srodes 1998, 14). See also 15 U.S.C. sec. 4901–4911 (1998); 15 U.S.C. secs. 175–176, 178, 182 (1997).

(1343). The result—and often the purpose—is a profound erosion of individual autonomy.

In this article, I focus on central government data-collection programs that share one defining characteristic: they compel production, retention, and dissemination of personal information about every American citizen.¹ Their target is ordinary American citizens carrying out ordinary day-to-day activities. Although these programs by no means constitute the whole universe of federal data collection, they are today the government's most critical informational levers for institutionalizing government control, individual dependence, and unprecedented threats to American liberties. Even within this circumscribed sphere, the immense volume of federal data collection defies brief summary. Accordingly, I confine the present inquiry to government development and recent expansion of

- Databases keyed to Social Security numbers—examining unchecked use of those numbers as a fulcrum for government data collection about individuals, and probing current legislative efforts to establish a national identification card;
- Labor databases—revealing new 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 the “unique health identifier” and implementation of the national electronic database of personal medical information mandated by the 1996 Health Insurance Portability and Accountability Act;
- Education databases—revealing federal databases mandated by the 1994 Goals 2000 Act, Improving America's Schools Act, and related legislation that establish detailed national records of children's educational experiences and socioeconomic status;
- 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.

Largely linked through an individual's Social Security number, these databases now empower the federal government to obtain an astonishingly detailed portrait of any person: the checks he writes, the types of causes he supports, 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. In this case, as in others, backers of these measures, in their effort to minimize resistance, predictably use political transaction-cost manipulation to that end, increasing the transaction costs to private individuals of perceiving—and taking

collective action to resist—governmental encroachments (Twight 1988, 1994). There is always an asserted benefit to be obtained, a plausible cover story.

The ostensible reasons have been diverse. With the spread of government-mandated use of Social Security numbers for database after electronic database, we have been told that it will reduce fraud—tax fraud, welfare fraud, the usual litany. With government assertion of the power to require businesses to contact the government for approval before hiring anyone, we have been told that it will help in cracking down on illegal immigration. With regard to government mandates for private physicians to record what we say to them in confidence, we have been told that it will reduce health-care fraud, promote efficiency, allow better emergency treatment, make it easier for the patient to keep track of his medical records, and the like. To rationalize government assertion of power to track what public school teachers record concerning our children, we have been told that it will assist in students' selection of a "career major," enhance assessment of school courses, and facilitate identification of students needing help. With government assertion of power to require banks to keep microfilm of all the checks we write, we have been told that it is to "reduce white-collar crime" and "inhibit money laundering." Who could oppose such worthy goals unless he had 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 administering them effectively and responsibly necessitates functions such as "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 extend the central government's purview even further.

Political transaction-cost manipulation has framed the issue in other ways besides these appealing rationales. In some cases discussed later, the database maneuvers were deliberately obscured from public view by means of what Claire Wolfe (1997) calls "land-mine legislation" that people don't notice until they step on it. 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 policy making. Information-law scholar Simon Davies (1994) judged the public's "greater acceptance of privacy-invasive schemes" to be in part a result of "proposals . . . being brought forward in a more careful and piecemeal fashion" that may be "lulling the public into a false sense of security."

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 so 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” (Davies 1994). Less than sixty years ago, race-based government roundups of law-abiding citizens also occurred in America, similarly facilitated by government data collection. As Solveig Singleton (1998a) and others have reported, “In the U.S., census data were used to find Japanese-Americans and force them into camps,” 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.”² By 1998, however, the events of the 1940s have become only a “vague memory”—and, except for the elderly, not a living memory at all (Davies 1994).

So today Congress proceeds apace. Having exposed most areas of our lives to ongoing government scrutiny and recording, Congress is now 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” (Davies 1994). The next generation awaits the full flowering of those 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”³

The Social Security number (SSN) has become the key to detailed government portraiture of our private lives. Even the Secretary of Health and Human Services (HHS) now describes American Social Security numbers as a “de facto personal identifier” [U.S. Dept. of HHS 1998, Section III(A)(1)]. Kristin Davis, senior associate editor for *Kiplinger’s Personal Finance Magazine*, recently described “the growing use of social security numbers as an all-purpose ID” as the “single biggest threat to protecting our financial identities” (quoted in Miller 1998). Since the Social Security

2. See also Singleton (1998b). The 1990 U.S. Census form 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, in 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).

3. Schwartz 1992, 1356, n. 165.

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 Social Security numbers 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 D. Roosevelt (1943) began the process with his executive order that subsequently, 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.

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 personnel 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. (Minor 1995, 262–63; footnotes omitted)⁴

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

The Privacy Act of 1974 did not stop the flood.⁵ Although purporting to restrict federal dissemination of SSNs, not only did it exempt existing federal SSN use

4. See also Pear 1998. 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 (letter of June 11, 1986).

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

previously authorized by statute or regulation, but it 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 notion of restricting SSN use and dissemination, Congress included in the 1976 tax reform act 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.⁶

On top of the far-reaching use of SSNs thus authorized, Congress continued to press for more.

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 at about age sixteen. Today every child must acquire an SSN at birth or shortly thereafter. How did policy makers accomplish such a radical change? Much as one conditions dogs: a bit at a time, and always with a reward attached. First, members of Congress required by statute in 1986 that every child claimed as a dependent on federal tax forms have an SSN by age 5. Then in 1988 Congress reduced the requirement by statute to age 2; in 1990 to age 1. Finally, in 1996, Congress passed a global requirement that an SSN must be presented for anyone of any age claimed on federal tax forms as a “dependent.” No SSN, no federal tax exemption. The Department of HHS reported that “beginning with tax returns filed 1/1/98 or later, the SSNs of all dependents claimed by a taxpayer must be included on the tax return” [U.S. Dept. of HHS 1998, Section III(A)(3)]. In general, to obtain any federal benefit, tax-related or otherwise, today one must present the Social Security numbers of all parties affected.⁷ To facilitate assignment of SSNs at birth, the federal government has financed state programs to secure issuance of the numbers as part of the birth-certificate registration process, an enticement that has enabled the Social Security Administration to secure adoption of its “Enumeration at Birth” process in all fifty states.

6. *Tax Reform Act of 1976*, Public Law 94-455 (October 4, 1976), 90 Stat 1525, at 90 Stat. 1711–1712. This law also made mandatory use of the SSN for federal tax purposes a matter of statutory law rather than IRS regulation. See Minor (1995, 264–65) on this point.

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 governing 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 a national electronic database 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 later discussed separately. First I consider the driver's license, birth certificate, and tamper-resistant Social Security card provisions.

The unprecedented federal assertion of control over state-issued drivers' licenses is buried in an omnibus bill, the 749-page Omnibus Consolidated Appropriations Act of 1997, which includes the "Illegal Immigration Reform and Immigrant Responsibility Act of 1996" (the "Immigration Reform Act"), the statute containing the relevant language.⁸ The key provisions begin 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 are difficult to spot even when you already know they are there.

Section 656(b) of the Immigration Reform Act deals with "State-Issued Drivers Licenses and Comparable Identification Documents." Cleverly conceived, it specifies that a "Federal agency may not accept for any identification-related purpose a driver's license or other comparable identification document, issued by a State, unless the license or document satisfies" federal requirements. The language thus makes compliance mandatory without saying so. Instead of telling the states "you must," it makes it

7. See, for example, Public Law 105-34 (August 5, 1997), Title X, sec. 1090(a)(2), (4), 111 Stat. 961, 962, 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" (emphasis added). See also 42 U.S.C. secs. 651-652 for relevant AFDC provisions.

8. *Omnibus Consolidated Appropriations Act, 1997*, Public Law 104-208 (September 30, 1996), 110 Stat. 3009; *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, Public Law 104-208, Division C (September 30, 1996), 110 Stat. 3009-546 ff.

nearly impossible for state residents to interact with the federal government if the state does not comply. The charade of voluntariness is buttressed by hard cash—grants to states “to assist them in issuing driver’s licenses and other comparable identification documents that satisfy the requirements” promulgated by the federal government.

Compliance requires the states to follow federal Department of Transportation regulations specifying both the form of the license and what constitutes federally acceptable “evidence of identity” in issuing the license. Raising the specter of biometric identifiers, it requires “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 mandates that in general “the license or document shall contain a social security account number that can be read visually or by electronic means.” States can 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 is readily at hand, mandated by the federal government—and easily linked electronically to any alternative identifier a state may adopt. Proposed federal Department of Transportation rules implementing these provisions already have been published.⁹

The other prong of the new federal control over state-issued identification documents entails regulation of the states’ issuance of birth certificates. The tactic is the same, requiring that a “Federal agency may not accept for any official purpose a certificate of birth” unless the birth certificate complies with federal regulations specifying “appropriate standards for birth certificates.”¹⁰ Bribes follow in the form of “grants to States to assist them in issuing birth certificates that conform to the standards set forth in the regulation.” Federal grants also are authorized for states “to assist them in developing the capability to match birth and death records” and to finance demonstration projects showing the feasibility of mandatory reports to “establish the fact of death of every individual dying in the State within 24 hours of acquiring the information.” An explicit objective is to “note the fact of death on the birth certificates of deceased persons.” However fleeting, the sole federal concession is to “not require a single design to which birth certificates issued by all States must conform” and to “accommodate the differences between the States in the manner and form in which birth records are stored and birth certificates are produced from such records.” The substance is another matter.

9. U.S. Dept. of Transportation (1998). In a passage that would make the Framers’ blood boil, the Department of Transportation’s explanation of the proposed rule notes that “States must *demonstrate compliance* with the requirements of the regulation by submitting a certification to the National Highway Traffic Safety Administration” (emphasis added).

10. *Illegal Immigration Reform and Immigrant Responsibility Act of 1996* [hereafter 1996 Immigration Reform Act], Public Law 104-208, Division C (September 30, 1996), 110 Stat. 3009-546 ff., at 110 Stat. 3009-716, sec. 656(a).

Perhaps the most ominous of Congress's innocuously titled "Improvements in Identification-Related Documents" requires the development of "prototypes" of a "counterfeit-resistant Social Security card."¹¹ 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 recurs in government discussions of the "unique health identifier" for medical records.¹² And these changes are aimed not just at people newly entering the Social Security system. The statute requires 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" (1996 Immigration Reform Act, sec. 657). The 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.¹³ 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 despite periodic statutory lip service to individual privacy. One example is the Social Security Administration (SSA) itself. 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.¹⁴

11. *Ibid.*, sec. 657. Virtually identical language was included in Public Law 104-193 (August 22, 1996), section 111, 110 Stat. 2105 ff.

12. Miller and Moore (1995) reported 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 five dollars each.

13. H.R. 231 (January 7, 1997), 105th Congress, 1st Session, 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 states: "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."

And, of course, the IRS. “Information” is defined to mean “information about an individual” that “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.¹⁵

Even without the Social Security Administration’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, Schwartz (1992) states 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 adds:

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. (1357)

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

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

15. *Ibid.*, sec. 401.25.

A similar pattern is evident in the federal Child Support Enforcement program. As Schwartz has recounted, after the program's creation in 1974, officials were granted access to ever more government databases of personal information. 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" (1367). Thereafter they gained access to IRS records and expanded the data-matching program to all families, making even non-AFDC families subject to "data matching and tax interception with the IRS." Schwartz quotes a state director of Child Support Enforcement as saying, "Some people would say that's Big Brotherism. Well, it is."¹⁶ Every child-support enforcement unit (CSEU) has access to all the AFDC data just listed as well as the Federal Parent Locator database. The Federal Parent Locator 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 forms; and commercial credit bureaus. The parent locator also allows searches of state data bases, three states at a time" (Schwartz 1992, 1369, footnotes omitted).

Pervasive government extraction of personal data that are stored and linked via compulsory use of SSNs is today's reality. 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 (1997) correctly stated in his testimony on a related bill, if it "looks like a duck, . . . quacks like a duck, . . . walks like a duck. . . . it's a duck."

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-curtailling federal powers Congress demands. So far the strategy has worked.

16. Schwartz 1992, 1367, 1369. Schwartz cites Jerrold Brockmyre, Director, Michigan Office of Child Support Enforcement, as quoted in Nancy Herndon, "Garnish: Dad," *Christian Science Monitor*, November 28, 1988, p. 25.

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 U.S. 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."¹⁷

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 (P.L. 104-193).¹⁸ For the stated purposes of preventing welfare fraud and enforcing child-support obligations, the law established an electronic database called a Directory of New Hires 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 Directory of New Hires nor the National Directory of New Hires is limited in any way to individuals receiving public assistance or to individuals paying or receiving child support. Instead, the new databases cover every working individual in America who enters the workforce or changes jobs.¹⁹ The journalist Robert Pear (1997) 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."

The 1996 law [P.L. 104-193, sec. 313(b)] 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." 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. 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" (P.L. 104-193, sec. 311).

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

18. *Personal Responsibility and Work Opportunity Reconciliation Act of 1996*, Public Law 104-193 (August 22, 1996), 110 Stat. 2105.

19. 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."

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 “information comparison services” is mandated. Access to the new hires database is explicitly granted to the Secretary of the Treasury (IRS), and the Social Security Administration 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 (P.L. 104-193, secs. 311, 316, 317).

Other major changes in 1996 came via the “Illegal Immigration Reform and Immigrant Responsibility Act of 1996” (P.L. 104-208). Although its most ominous provisions are cast as “pilot programs,” their scope and structure clearly indicate the direction of things to come. Using the rationale of controlling illegal immigration, this 1996 statute establishes pilot programs requiring employers to seek the central government’s certification of a person’s “work authorization” before making final an offer of employment. And the manner in which the federal government’s approval is to 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 is Congress’s mandate that the U.S. Attorney General establish a pilot “employment eligibility confirmation system,” keyed to information provided by the Social Security Administration 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 hires that person. As John J. Miller and Stephen Moore (1995) described such proposals prior to passage of the pilot-program law, “In other words, the government would, for the first time in history, require employers to submit all of their hiring decisions for approval to a federal bureaucrat.” Although individual firms’ election to participate is at present voluntary, the reward for participating is protection from both criminal and civil liability for “any action taken in good faith reliance on information provided through the confirmation system” (P.L. 104-208, sec. 403).

The three pilot programs reflect increasing proximity to a national identification-card system. The “basic” program requires 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” (P.L. 104-208, sec. 401). 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 requires 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 individual” [P.L. 104-208, sec. 403(a)]. If the firm continues to employ the individual after a “final nonconfirmation” of work eligibility through the federal electronic database system, the statute creates a rebuttable presumption that the firm has violated a provision of immigration law that carries civil penalties of as much as \$2,000 per unauthorized hire on the first offense and as much as \$5,000 or \$10,000 for subsequent offenses.²⁰

With the “Citizen Attestation Pilot Program,” linkages with other facets of the coordinated federal data expansion effort become 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, requiring each state driver’s license to contain both a photograph and “security features” that render it “resistant to counterfeiting, tampering, and fraudulent use.”²¹ 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” comes even closer to a national-identity-card approach. With one major exception, it follows the basic pilot program. To participate in the machine-readable document pilot program, a state must have adopted a driver’s license format that includes a “machine-readable social security account number.” Participating firms “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 [P.L. 104-208, sec. 403(c)]. 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, includes a provision headed “No

20. P.L. 104-208, at 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).

21. P.L. 104-208, sec. 403(b), 110 Stat. 3009-662 ff. See also sec. 656(b) of the same act, 110 Stat. 3009-718, discussed earlier (“state-issued drivers licenses and comparable identification documents”).

National Identification Card” that proclaims that “nothing 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” [P.L. 104-208, sec. 404(h)]. Such provisions, appearing ever more frequently in federal legislation, merely highlight the clear and present danger of exactly the type of system disavowed.

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 the bill, Stephen Moore (1997, 2–3) 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.

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

Vastly more was poured into it in 1998. The Workforce Investment Act 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, the 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 reassures us that this vast array of information will remain “confidential.”²²

Behind nomenclature that continues to conceal more than it reveals to ordinary Americans, government pressure thus persists for an ever-increasing repository of per-

sonal information to fatten and consolidate national employment databases and identification systems. The Workforce Investment Act and the federal pilot work-authorization program move in that direction, taking 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” (1997, 2).²³ The objectives of 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 new federal mandate for a unique nationwide health identifier for each individual, to be used in a national electronic database of personal medical information. People familiar with the proposed encroachments find few words strong enough to impart the magnitude of the threat to personal privacy. Although the federal government already has access to millions of medical records through Medicare, Medicaid, and the newly authorized federal subsidies for State Children’s Health Insurance Programs, the national electronic database of health information authorized by the Health Insurance Portability and Accountability Act of 1996²⁴ (HIPAA, P.L. 104-191) involves the government in everyone’s health care, whether or not they receive federal subsidies (Twight 1998). Steve Forbes (1997) has described it as a “breathtaking assault on the sanctity of your medical records.” Ellyn Spragins and Mary Hager (1997) noted the “big, ugly fact” that under the 1996 act “every detail of your medical profile may well land in this new system without your consent,” explaining that the new national databank will allow “anyone who knows your special health-care number” to become “pry to some of your most closely guarded secrets.”

Despite such occasional outcries, even today neither the public nor the media have fully awakened to the scope of the 1996 law. In fact, 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

22. *Workforce Investment Act of 1998*, Public Law 105-220 (August 7, 1998), 112 Stat. 936 ff., at sec. 309, 112 Stat. 1082-1083; emphasis added.

23. Moore 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.”

24. *Health Insurance Portability and Accountability Act of 1996*, Public Law 104-191 (August 21, 1996), 110 Stat. 1936ff.

was mandated by statutory law was described elsewhere in the media as “breaking news” (Stolberg 1998a). 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.” Yet, for two years hardly anyone had paid heed to those provisions of statutory law.

Meanwhile the federal bureaucracy proceeded systematically to carry out its statutory duty to select a health identifier. On July 2, 1998, the U.S. Department of Health and Human Services released a lengthy White Paper entitled “Unique Health Identifier for Individuals.” In that chilling document, HHS calmly discussed exactly what Orwellian form the “unique health identifier” will take, what degree of encroachment on individual privacy will be compelled. HHS considered six alternatives 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; and Public Key-Private Key Cryptography Method.” As HHS stated, “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 in the push to expand government data collection recurred here, augmented in this case 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” [U.S. Dept. of HHS 1998, sec. III(A)]. 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 the perspective of political transaction-cost manipulation, that proposal holds appeal, for it would give the appearance of individual control without the reality. (Does anyone think that there would not 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” because “a request for the identifier might be interpreted to mean that the individual has something to hide”! HHS also was troubled by the proposal because of the department’s

“anticipat[ion] that, given the choice, significant numbers of individuals would request the alternate identifier” [U.S. Dept. of HHS 1998, secs. III(B)(1)–III(B)(3)].

Equally stunning are proposals to require biometric identifiers as the unique health identifier. The HHS White Paper describes 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 are chiefly mechanical obstacles—that “no infrastructure” now exists to support such identifiers, that the necessary “special equipment” would “add to the cost” of this alternative, and the like [U.S. Dept. of HHS 1998, sec. III(C)(2)]. 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 loss of liberty or threat of a police state, unless those issues inhered in the reference to “linkages that would be punitive.”

Another alternative presented 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.” The 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.” [U.S. Dept. of HHS 1998, sec. III(C)(4)]. 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.

One proposal that elicited strong HHS support was a hybrid proposal called “Universal Healthcare Identifier/Social Security Administration” (UHID/SSA). The UHID is an identifier as many as twenty-nine characters long involving a sixteen-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” (U.S. Dept. of HHS 1998, sec. III(E)(1)).

There is more, including some less intrusive measures, but these excerpts convey the spirit of this shocking document. Although HHS “welcome[s] comments” on the alternative health identifiers, absent congressional reversal of the underlying statutory mandate the die is largely cast. However, as implementation approaches, greater efforts will be made to soothe the public. Such efforts were apparent in HHS’s disingenuous reference to consumers’ “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”—proclaimed in November 1997 by the President’s Quality Commission. No one knowledgeable of the electronic-database provisions of the 1996 Health Insurance Portability and Accountability Act has objective grounds for believing such rights to be secure any longer under existing statutory law. Indeed, the HHS White Paper itself stated 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” [U.S. Dept. of HHS 1998, secs. II(B), II(C)]. Given the predilections of federal officials and the proposals at hand, the problem is quite the opposite.

Yet the effort to soothe continues. In late July 1998, after the *New York Times* had publicized the issue, federal officials took steps to distance themselves from the unique health identifier. It was a remarkable display, given that the very language of the statutory provisions involved—including the lack of privacy restrictions—was a Clinton administration creation first unveiled in the reviled 1993 Health Security Act. Nonetheless, on July 31 Vice President Al Gore ceremoniously proclaimed a new White House commitment to a multifaceted “Electronic Bill of Rights” supposed to include, 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 (White House Press Release 1998).²⁵

However, if Congress does not pass privacy measures by August 21, 1999, HHS is statutorily bound to proceed. The 1996 legislation stated:

If legislation governing standards with respect to the privacy of individually identifiable health information . . . is not enacted by the date that is 36

25. See also Simons (1998); Stolberg (1998b); Brinkley (1998).

months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. [P.L. 104-191, sec. 264(c)(1)]

The language mandating unique health identifiers was equally 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 (P.L. 104-191, sec. 262(a), sec. 1173). Unless statutory provisions now mandating the national electronic database and “unique health identifiers” are repealed, both will become realities, regardless of the source or efficacy of privacy restrictions and despite predictable political posturing.

Once the medical information is assembled, its likely uses and constituencies will multiply. As early as June 1997, Spragins and Hager reported that “organizations 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 scope of the centralized information. Already the National Committee on Vital and Health Statistics has “tentatively recommended that this mother lode of medical information be further augmented by specifics on living arrangements, schooling, gender and race.”

The issue is not just privacy; it is government power. Assessing the impact of the new national database and unique health identifiers, Dr. Richard Sobel of Harvard Law School understood that aspect clearly: “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” (quoted in Stolberg 1998a, A13). 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 permeates our educational system, its scope expanded by the 1994 legislation mentioned earlier. As with medical and employment information, in the education system individually identified information is being centralized in linked national electronic databases, 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 several Fairfax County school board members “challeng[ed] a planned \$11 million computer database that would let schools com-

pile 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.” The *Washington Post* reported that 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 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” (Robberson 1997).

That nationwide data-exchange network—orchestrated by the federal government and extended through the 1994 Goals 2000: Educate America Act; the Educational Research, Development, Dissemination, and Improvement Act; the School-to-Work Opportunities Act; and the Improving America’s Schools Act—is now 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.

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.²⁶ Included within the Office of Educational Research and Improvement are the National Center for Education Statistics, five “national research institutes,”²⁷ 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.”²⁸ 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 the U.S. Department of Education.

26. *Educational Research, Development, Dissemination, and Improvement Act of 1994*, Public Law 103-227, Title IX (March 31, 1994), 108 Stat. 212 ff., sec. 912.

27. 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.

28. *Ibid.*, sec. 912.

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 the Education Department 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 the Department of Education “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.²⁹ Through the School-to-Work Opportunities Act the Labor Department also participates in the data endeavor, its Secretary required to act jointly with the Secretary of Education 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.”³⁰

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”), the federal entity most directly and extensively involved in receiving individually identifiable information about American children and their education.

The National Center has statutory authority to “collect, analyze, and disseminate statistics and other information relating to education” in the United States and elsewhere.³¹ It is specifically authorized to collect data on such subjects 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 9, 13, and 17 and in grades 4, 8, and 12 in public and private schools” (P.L. 103382).³² States participating in the NAEP testing process thus generate additional individually identified student information for the federal government.

29. *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.

30. *School-to-Work Opportunities Act of 1994*, Public Law 103-239 (May 4, 1994), 108 Stat. 568 ff., sec. 404.

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

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 the Department of Education 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.³³

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” (P.L. 103-382, sec. 411). The question is, do these provisions guarantee the security of such personal information?

Unfortunately, they do not. 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 (P.L. 103-382, sec. 408). 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 [P.L. 103-382, sec. 408(b)(7)]. Separate Department of Education privacy regulations also countenance myriad disclosures without the consent of

32. *National Education Statistics Act of 1994*, Public Law 103-382, Title IV (October 20, 1994), 108 Stat. 4029 ff., sec. 404 (“violence”), sec. 411 (“grades 4, 8, and 12”).

33. *Ibid.*, sec. 405 (“may consider appropriate”), sec. 410 (“uniform information”).

the subject individuals, among them disclosures made for “routine uses” (one of the major loopholes in the 1974 federal Privacy Act discussed earlier) and those made to another government agency “for a civil or criminal law enforcement activity” authorized by law, and to either house of Congress or to “any committee or subcommittee thereof” with relevant subject-matter jurisdiction.³⁴

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 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 approved purposes.³⁵ 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 the lawmakers intended.

But disclosures beyond those intended by lawmakers 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 comes to mind again: giving a teenager keys to a motorcycle, handing him a bottle of liquor, and admonishing him not to drink and drive. Once again we’re asking for trouble. Even criminal penalties authorized for individuals convicted of violating confidentiality provisions of the laws do little to assuage legitimate privacy concerns.

Nonetheless, although on one level the shell of protection around this reservoir of personal information is extremely porous, on another level it is dangerously tight.

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

35. *Family Educational Rights and Privacy Act*, Public Law 93-380, Title V, sec. 513 (August 21, 1974), 88 Stat. 571, as amended. 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).

With respect to administrative and judicial review, legislators have built a statutory firewall around the information and its collection—a provision seemingly designed to block ordinary legal oversight while giving nearly total discretion to the Commissioner of Education Statistics. The statute states:

No collection of information or data acquisition activity undertaken by the Center shall be subject to any review, coordination, or approval procedure except as required by the Director of the Office of Management and Budget . . . except such collection of information or data acquisition activity may be subject to such review or coordination if the Commissioner determines that such review or coordination is beneficial.³⁶

By placing vast discretion regarding collection and distribution of personal information in the hands of a single individual, and by largely preventing citizens from blocking transfer of such 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" (quoted in Robberson 1997).

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

Privacy in America is further jeopardized by federal statutory law now 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 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 those intrusions and the 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 (P.L. 91-508).³⁷ 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

36. *National Education Statistics Act of 1994*, Public Law 103-382, Title IV (October 20, 1994), 108 Stat. 4029 ff., sec. 408(b)(4). See also sec. 408(a)(1), which states "No person may . . . permit anyone other than the individuals authorized by the Commissioner to examine the individual reports."

37. Public Law 91-508, Title I (October 26, 1970), 84 Stat. 1114. The FDIC's notice of proposed rulemaking may be found in *Federal Register*, Vol. 63, No. 234 (December 7, 1998), pp. 67529–67536. Withdrawal of that notice by the FDIC was announced in: *Federal Register*, Vol. 64, No. 59 (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.

- (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. . . . (P.L. 91-508, sec. 101)

That requirement entailed microfilm records of every detail of every customer's bank account—each check, each deposit—with each account identified by the holder's Social Security number.³⁸ The statute authorized similar record-keeping to be required of uninsured institutions, including even credit-card companies (P.L. 91-508, sec. 123). Putting further discretionary power in the hands of the Treasury secretary, a 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.”³⁹ 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.⁴⁰ 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 the banks' records were disclosed to the government as evidence through compulsory legal process. The Court stated that “claims of depositors against the compulsion by lawful process of bank records involving the depositors' own transactions must wait until such process issues” (416 U.S. 51-52). Dissenting, Justice 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

38. 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.

39. The *Currency and Foreign Transactions Reporting Act* constituted Title II of the same statute: Public Law 91-508, 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, see Pilon 1998 and Bovard 1997.

40. *California Bankers Association v. Shultz*, 416 U.S. 21, 39 L.Ed.2d 812, 94 S.Ct. 1494 (April 1, 1974).

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. (416 U.S. 96-97)

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,

calling 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" (416 U.S. 97).

Justice Marshall's "hollow charade" assessment was vindicated two years later by the Court's 1976 decision of *United States v. Miller*.⁴¹ Stating flatly that depositors have "no legitimate 'expectation of privacy'" in their bank records, the Court 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 (425 U.S. 442-43). 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.⁴² 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.⁴³

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.⁴⁴ That certification may be based on any of the listed rationales, including a federal official's "formal written request," the lenient

41. 425 U.S. 435, 48 L.Ed.2d 71, 96 S.Ct. 1619 (April 21, 1976).

42. *Right to Financial Privacy Act*, Public Law 95-630, Title XI (November 10, 1978), 92 Stat. 3697 ff., codified to *U.S. Code*, Title 12, sec. 3401 ff.

43. *Ibid.*, sec. 3402.

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 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 simply by 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 from the date when the request was mailed, 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."⁴⁵ 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.⁴⁶ In addition, the act allows government authorities to obtain emergency access to financial records from banks and other financial institutions if they declare that "delay in obtaining access to such records would create imminent danger of—(A) physical injury to any person; (B) serious

44. 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.

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

46. *Ibid.*, sec. 3413. These include, inter alia, 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.

property damage; or (C) flight to avoid prosecution,” provided that the government authority subsequently files in court a sworn statement by a supervisory official and provides notification as specified in the act.⁴⁷

These exceptions, along with the porosity of the statute’s strictures, make the Financial Privacy Act weak grounds for protection from unwarranted federal scrutiny of personal bank transactions. No surprise. Surely we 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. As obliging Congresses cobble together loose statutes such as the Right to Financial Privacy Act, we now know that even such porous protections can 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 bank records now threatening our financial privacy are unlikely to provide reliable protection.

Government as Privacy Protector?

In 1974 Congress passed the omnibus Privacy Act, cited earlier in this article, 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 following “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 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

47. *Ibid.*, sec. 3414(b). Moreover, the Financial Privacy Act does not apply to state or local government attempts to gain access to these records. See *U.S. v. Zimmerman*, N.D. W.Va., 957 F.Supp. 94 (1997).

Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.⁴⁸

Despite that clear acknowledgment of the federal threat to personal privacy, the 1974 Privacy Act—riddled with exceptions and counterbalanced by disclosure mandates in the Freedom of Information Act⁴⁹—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” (quoted in Prowda 1995, 749–50).

No stronger proof of the act’s failure could be given than the fact that all of the privacy-destroying measures discussed in this article 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 a national electronic database 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 intrusions now coexist with a law ostensibly assuring our privacy vis-à-vis the federal government’s “collection, maintenance, use, and dissemination” of personal information.

In 1988, as people became increasingly alarmed about government centralization of personal information, Congress sought to strengthen the Privacy Act by adding the “Computer Matching and Privacy Protection Act.”⁵⁰ 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 matching provided that a “computer matching program” was “pursuant to a written agreement between the source agency and the recipient agency” that met specified procedural requirements. Recent federal database matching activities through the “new hires” database, pilot programs for work authorization, child-support enforcement programs, and other programs confirm that the 1988 act provided scant impediment to the ongoing federal data quest.

Today, federally required databases of personal information continue to proliferate. One measure of their current scope is that, in the Code of Federal Regulations, the

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

49. Public Law 89-554 (September 6, 1966), 80 Stat. 383, as amended. Codified to *U.S. Code*, Title 5, sec. 552 (1998).

50. Public Law 100-503 (October 18, 1988), 102 Stat. 2507-2514, sec. 2. Codified at *U.S. Code*, Title 5, sec. 552a(o).

index entry under the heading “Reporting and recordkeeping requirements” is itself sixty-two pages long! Information on such a scale would not be collected unless federal officials planned to use it to change private behavior—social behavior, economic behavior, political behavior. Far from innocuous, this data collection and the intensity of its pursuit reveal the enormous value placed on such intelligence by federal officials. Representative Jim McDermott (D., Washington), one of the few members of Congress who actively resisted the 1996 authorization of a national electronic database for health care, recently 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” (quoted in Stolberg 1998a, A13).

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 an IRS commissioner who “is a ruthless son of a bitch, that he will do what he’s told, that every income tax return I want to see I see, that he will go after our enemies and not go after our friends” (quoted by Wall Street Journal Board of Editors 1997). It has been widely reported that Democratic President Bill Clinton, for similar reasons, apparently sanctioned illegal transfer of nine hundred or more FBI files to the White House. And, ironically, federal agencies such as the IRS have routinely used privacy legislation to shield evidence of their own misdeeds (Davis 1997, 164–68). 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 Sobel’s succinct observation that “centralized information is centralized power” (Stolberg 1998a, A13).

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, Solveig Singleton (1998a) proposed a better way to protect privacy:

The better model for preserving privacy rights and other freedoms in the United States 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 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.

Of course, the Founders tried to hold back the power of government through the U.S. Constitution. As H. L. Mencken ([1940] 1990) 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. (350)

As I have shown elsewhere (Twight 1988, 1994), that 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 Alfred J. Nock's ([1939] 1991) insight that "whatever power you give the State to do things for you carries with it the equivalent power to do things to you" (274). 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 the 1996 Health Insurance Portability and Accountability Act, despite outspoken efforts in 1996 by Representative McDermott and several other legislators to publicize the extraordinary threat to privacy contained in the provisions for a national electronic database, 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 "members of Congress did not recognize the privacy implications of what they had done until media reports about the issue came out this week" (Associated Press 1998).

So easily assuaged, so vulnerable to political transaction-cost manipulation, individuals who prize liberty and privacy even now are celebrating a spurious victory regarding the unique health identifier, apparently comforted by Vice President

Gore's commitment to an "Electronic Privacy Act." But Gore's own press release, though it notes a raft of new controls the administration would like to place on private businesses' use of personal information, is nearly silent regarding *government* use of personal information, stating only an intention to "launch a 'privacy dialogue' with state and local governments" that will 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" (White House Press Release 1998). With existing statutes and regulations usurping personal privacy more aggressively with each passing day, it is much too late for a bureaucratically mired "privacy dialogue."

Those invasive statutes and regulations are today's reality. The government data collection they now authorize would have seemed unimaginable in an America whose citizens once boldly, meaningfully proclaimed individual freedom. Indeed, what important personal information is *not* now at the fingertips of curious federal officials? Centralized power is centralized information, and 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" (Schwartz 1995, 307; footnote omitted).

Reducing central government power is the only alternative to such helpless dependence. Whether that alternative can be realized is a more complex question. As government data-collection mandates proliferate and encryption issues loom larger, those who cling to government as privacy's bulwark might well reflect on John Perry Barlow's statement that "trusting the government with your privacy is like having a peeping Tom install your window blinds."⁵¹ As Bernadine Healy (1998) wrote regarding unique health identifiers and the national medical-record database, the "Government does a lot of things well, but keeping secrets is not one of them."

References

- Associated Press. 1998. Congress Won't Delay Medical Identification Law. Posted by Cable News Network (www.CNN.com), July 23.
- Bovard, James. 1997. The Dangerous Expansion of Forfeiture Laws. *Wall Street Journal*, December 29, p. A11.
- Brinkley, Joel. 1998. Gore Outlines Privacy Measures, but Their Impact Is Small. *The New York Times on the Web*, August 1.

51. John Perry Barlow, co-founder of the Electronic Frontier Foundation, is quoted in Prowda 1995 (765, citing Jeff Rose, "Right to E-mail Privacy Would Seem Self-Evident," *San Diego Union Tribune*, March 1, 1994 [Computerlink], p. 3, as the source of the Barlow quotation).

- Davies, Simon G. 1994. Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine. *Information Technology & People* 7 (4).
- Davis, Shelley L. 1997. *Unbridled Power: Inside the Secret Culture of the IRS*. New York: HarperCollins.
- Forbes, Steve. 1997. Malpractice Bill. *Forbes*, October 6, p. 27.
- Gupte, Pranay, and Bonner R. Cohen. 1997. Carol Browner, Master of Mission Creep. *Forbes*, October 20, pp. 170–77.
- Healy, Bernadine. 1998. Hippocrates vs. Big Brother. *New York Times*, July 24, p. A21.
- Mencken, H. L. 1940. The Suicide of Democracy. In *The Gist of Mencken: Quotations from America's Critic*, edited by Mayo DuBasky. Metuchen, N.J.: Scarecrow Press, 1990.
- Miller, John J., and Stephen Moore. 1995. A National ID System: Big Brother's Solution to Illegal Immigration. *Cato Policy Analysis* no. 237 (September 7). Washington, D.C.: Cato Institute (<http://www.cato.org>).
- Miller, Theodore J. 1998. Look Who's Got Your Numbers. *Kiplinger's Personal Finance Magazine*, July, p. 8.
- Minor, William H. 1995. Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections. *Columbia Journal of Law and Social Problems* 28 (2): 253–96.
- Moore, Stephen. 1997. A National Identification System. Testimony before the U.S. House of Representatives, Subcommittee on Immigration and Claims, Judiciary Committee, May 13. (Available on the Internet at <http://www.cato.org/testimony/ct-sm051397.html>).
- Nock, Albert Jay. March 1939. The Criminality of the State. In *The State of the Union: Essays in Social Criticism*, edited by Charles H. Hamilton. Indianapolis, Ind.: Liberty Fund, 1991.
- Pear, Robert. 1997. Government to Use Vast Database to Track Deadbeat Parents. *The New York Times on the Web*, September 22.
- . 1998. Not for Identification Purposes. (Just Kidding.) *The New York Times on the Web*, July 26.
- Pilon, Roger. 1998. High Court Reins in Overweening Government. *Wall Street Journal*, June 23, p. A20.
- Prowda, Judith Beth. 1995. Privacy and Security of Data. *Fordham Law Review* 64: 738–69.
- Robberson, Tod. 1997. Plan for Student Database Sparks Fears in Fairfax. *Washington Post*, January 9, p. A01 (www.washingtonpost.com).
- Roosevelt, Franklin D. 1943. Executive Order 9397: Numbering System for Federal Accounts Relating to Individual Persons. *Code of Federal Regulations*, Title 3, pp. 283–84. November 22.
- Schwartz, Paul. 1992. Data Processing and Government Administration: The Failure of the American Legal Response to the Computer. *Hastings Law Journal* 43 (part 2): 1321–89.
- . 1995. The Protection of Privacy in Health Care Reform. *Vanderbilt Law Review* 48 (2): 295–347.
- Simons, John. 1998. Gore to Propose Consumer-Privacy Initiative. *Wall Street Journal*, July 31, p. A12.

- Singleton, Solveig. 1998a. Don't Sacrifice Freedom for "Privacy." *Wall Street Journal*, June 24, p. A18.
- . 1998b. Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector. *Policy Analysis* no. 295 (January 22). Washington, D.C.: Cato Institute.
- Spragins, Ellyn E., and Mary Hager. 1997. Naked before the World: Will Your Medical Secrets Be Safe in a New National Databank? *Newsweek*, June 30, p. 84.
- Srodes, James A. 1998. Protect Us from Environmental Protection. *World Trade*, July, pp. 14–15.
- Stolberg, Sheryl Gay. 1998a. Health Identifier for All Americans Runs Into Hurdles. *New York Times*, July 20, pp. A1, A13.
- . 1998b. Privacy Concerns Delay Medical ID's. *The New York Times on the Web*, August 1.
- Twight, Charlotte. 1988. Government Manipulation of Constitutional-Level Transaction Costs: A General Theory of Transaction-Cost Augmentation and the Growth of Government. *Public Choice* 56: 131–52.
- . 1994. Political Transaction-Cost Manipulation: An Integrating Theory. *Journal of Theoretical Politics* 6 (2): 189–216.
- . 1998. Medicare's Progeny: The 1996 Health Care Legislation. *Independent Review* 2 (3): 373–99.
- U.S. Department of Health and Human Services. 1998. Unique Health Identifier for Individuals: A White Paper. Washington, D.C.: U.S. Government Printing Office, July 2.
- U.S. Department of Transportation, National Highway Traffic Safety Administration. 1998. State-Issued Driver's Licenses and Comparable Identification Documents; Proposed Rule. *Federal Register* 63 (116), June 17, pp. 33219–33225; *Code of Federal Regulations*, Title 23, Part 1331.
- Wall Street Journal Board of Editors. 1997. Politics and the IRS. *Wall Street Journal*, January 9, p. A10.
- White House Press Release. 1998. Vice President Gore Announces New Steps toward an Electronic Bill of Rights. July 31.
- Wolfe, Claire. 1997. Land-Mine Legislation. 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).

Acknowledgments: This article is adapted from Charlotte Twight's forthcoming book, *Designing Dependence: The Rise of Federal Control over the Lives of Ordinary Americans*, to be co-published by the Cato Institute.