The Phyllis Schlafly Report

VOL. 31, NO. 12 | P.O. BOX 618, ALTON, ILLINOIS 62002 | JULY 1998

Liberty vs. Totalitarianism, Clinton-Style

Monitoring by I.D. and Database

Two of the principal mechanisms by which the rulers of 20th century police states maintained their control over their people were the *file* and the *internal passport*. These governments kept a cumulative file (called the *dangan* in Communist China) on every individual's performance and attitudes from school years through adult employment. Citizens carried an internal passport or "papers" that had to be presented to the authorities for permission to travel within the country, to take up residence in another city, or to apply for a new job.

These two methods of personal surveillance — efficient watchdogs that prevented any emergence of freedom — required an army of bureaucrats fortified by a Gestapo, a Stasi or a KGB, plus the ability to commandeer an unlimited supply of paper and file folders. Technology has now made the task of building personal files on every citizen, and tracking our actions and movements, just as easy as logging onto the Internet.

Unknown to most Americans, coordinated plans are well underway to give the Federal Government the power to input personal information on all Americans onto a government database. The computer will record our school, business, medical, financial, and personal activities, and track our movements as we travel about the United States.

These plans were authorized by the so-called conservative Congress and are eagerly implemented and expanded by the Clinton Administration liberals. They plan to force all Americans to carry an I.D. card linked to a federal database, without which we will not be able to drive a car, get a job, board a plane, enter a hospital emergency room or school, have a bank account, cash a check, buy a gun, or have access to government benefits such as Social Security, Medicare, or Medicaid.

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

Legislative authority for these dramatic changes in what we endearingly call the American way of life was buried in two bills passed by Republicans and signed by Bill Clinton in 1996: the Illegal Immigration Reform and Immigrant Responsibility Act, and the Personal Responsibility and Work Opportunity Reform Act (known as welfare reform).

The illegal immigration law prohibits the use of state driver's licenses after Oct. 1, 2000 unless they contain Social Security numbers as the unique numeric identifier "that can be read visually or by electronic means." (Section 656(b)) The act requires all driver's licenses to conform to regulations promulgated by the Department of Transportation, which published its proposed regulations on June 17. (*Federal Register*, vol. 63, no. 116, pp. 33219-33225)

The illegal immigration law orders the Attorney General to conduct pilot programs in at least 5 states where the state driver's license includes a "machine-readable" Social Security number. (Section 403(c)) The law also orders the development of a Social Security card that "shall employ technologies that provide security features, such as magnetic stripes, holograms, and integrated circuits." (Section 657(a)) A "smart card" with these technologies can contain a digitized fingerprint, retina scan, voice print, DNA print, or other biometric identifier, and will leave an electronic trail every time it is used.

The law orders "consultation" with the American Association of Motor Vehicle Administrators. AAMVA, a pseudo-private, quasi-government organization, has long urged using driver's licenses, with Social Security numbers and digital fingerprinting, as a de facto national I.D. card that would enable the government to track everyone's movements throughout North America.

The welfare reform law requires that, in order to receive federal welfare funds, states must collect Social Security numbers from applicants for any professional license, occupational license, or "commercial driver's license." (Section 317) The Balanced Budget Act of 1997, in the guise of making "technical corrections" to welfare reform, deleted the word "commercial," thereby applying the requirement to *all* driver's license applicants, and even added "recreational" (hunting and fishing) licenses.

Another provision of welfare reform requires employers, since Oct. 1, 1997, to transmit the name, address, and Social Security number of every new worker to a Directory of New Hires. This is supposed to help track

deadbeat dads, but the information is collected from *all* new workers (regardless of whether they are deadbeats or even dads) and maintained for 24 months.

The "instant background check" established by the 1993 Brady Act takes effect nationwide on Dec. 1. Under this system, prospective handgun buyers must be screened against a database of convicted criminals. But the new national I.D. card will make it easy to keep a database of gun buyers, too, which some states reportedly are doing already. Although the Brady Act forbids federal agencies from using the instant check system to register firearms, the FBI says it plans to keep records of prospective handgun buyers for 18 months.

A few states have already quietly legislated acquiescence in the new federal requirements, but fingerprinting and smart cards have stirred an uproar in others. Most Americans have never been fingerprinted and look upon it as something that happens only to criminal suspects.

The New Jersey Legislature recently abandoned efforts to pass Governor Christine Whitman's high-tech driver's license called "Access New Jersey." It was designed to contain a computer chip with 100 electronic keys capable of storing large amounts of personal data. It would leave an electronic trail each time the card was used to cash a check, make a purchase, pay a toll, check out a book, get insurance authorization to see a doctor, or used for identification, all identified by Social Security number.

These new federal laws effectively overturn the 1974 Privacy Act, which declared that "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his Social Security account number." On the pretext of catching illegal aliens, welfare cheats, deadbeat dads, and criminals, these laws will subject law-abiding Americans to the police-state apparatus of national I.D. cards linked to coordinated government databases.

Feds Grab for Medical Records

One of the major features of Bill and Hillary Clinton's nationalized health care plan, which the public rejected in 1994, was giving the Federal Government a database of every American's medical records. Each person was to have a Health Security Card (which Clinton waved for the cameras during his 1994 State of the Union Message) with a "unique identifier number" that would give government bureaucrats easy computer access to everybody's entire medical history.

The Clinton health plan included setting up a National Health Board, responsible only to the President, with extraordinary rulemaking powers to "assure uniformity" and to decide what may and may not be spent on health care, both globally and by each provider. Physicians and other providers were to be required to report every medical service to the national database.

The Card and the database were presented to the public, on the one hand, as each individual's personal key to free health care, and on the other hand, as a means of "health care planning" and of eliminating fraud among providers. The American people, however, easily recognized the Card and the database as bringing an end to medical privacy and as federal control over what health care we would be permitted to receive, with ultimate rationing by bureaucrats or gatekeepers.

Clinton failed to get his nationalized health bill passed in 1994, but he has been progressing toward the same goal incrementally through other legislation. Sometimes the bills are packaged as "for the kids" (*e.g.*, the 1997 Kidcare bill) and sometimes as "stop the fraud" (*e.g.*, the 1996 Health Insurance Portability and Accountability Act known as Kennedy-Kassebaum), but the bottom line is to require computerized reporting and to gather more and more information on government databases.

The Kennedy-Kassebaum law requires the Department of Health and Human Services to adopt standards for a "unique health care identifier" for each individual, as well as each employer, provider, and health plan. Everyone will have to submit an identification document with a unique number in order to receive health care, or the provider will not be paid.

The latest bait used by the Clintonian liberals to get all medical records on a federal database is the current drive to set up a federal Immunization Registry that will tag all children at birth and track them until death. This will achieve the original Clinton Administration goal of computerizing the health records of all Americans, with unique personal identifiers (Social Security numbers, if possible), in order to make us conform to government health policy.

The 1993 Comprehensive Child Immunization Act authorized the Secretary of Health and Human Services (HHS) "to establish state registry systems to monitor the immunization status of all children." HHS has since sent $417 million of taxpayers' money to the states to set up these databases, and this money has been supplemented by millions of dollars from the Robert Wood Johnson Foundation.

The 1998 Centers for Disease Control brochure on "Immunization Registries" explains the objective. CDC is "committed to promoting the development and maintenance of computerized registries as a key data resource" that will "fill the information gap" by furnishing the government with "consolidated records," "instant access," and "automated recall notifications."

CDC sees itself as a social change agent, engaging in massive grassroots lobbying (with taxpayers money, of course). The brochure boasts that, following Clinton's personal instructions to the Secretary of Health and Human Services, CDC is working to overcome public opposition. The brochure announces that CDC will be the catalyst "to build political will and consensus" for this health care registry and establish a time line for nationwide registry implementation.

The CDC admits it is working toward "integration of the immunization registry movement with the rapidly developing field of medical informatics, and promoting the inter-operability of registries with other developing medical information systems." Dr. Alan Hinman, former CDC official and now with the Jimmy Carter Presidential Center, stated publicly on May 14: "Immunization registries would be viewed in these settings as merely one aspect of the overall patient information system."

At least half the states have been putting children on state databases, often without their parents' knowledge or consent. Texas legislators discovered that the Texas Department of Health has built up an electronic database of 3.3 million Texas children, based on birth certificates and Social Security numbers, while ignoring the law's requirement for parental consent.

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

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

Don't be misled by the efforts in Congress to pass so-called privacy legislation that creates hundreds of new crimes and layers of new bureaucracies, supposedly to safeguard against unauthorized disclosure of confidential health information. Tell your Member of Congress that all HHS appropriation bills should forbid the spending of taxpayers' money to collect or coordinate medical information on individuals. Our medical records are none of the government's business.

Feds Want to Control Encryption

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

The Fourth Amendment to the Constitution, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," was written at time when unreasonable searches and seizures were carried out principally by armed troops. This language is just as applicable and vital today to protect us against unreasonable searches carried out by modern mechanisms.

Encryption is the marvelous technology that can enable us to have private phone conversations and send e-mail messages that are secure from prying eyes — just like sealing the envelope of a letter. Encryption is a code that makes your phone conversations and e-mail sound or look like gibberish to everyone except those to whom you give the key to decode them.

Encryption can enable American citizens to protect both our Fourth Amendment rights and our First Amendment right to speak or write in any language, whether English, Spanish, Greek, or code. Surely, American freedom should include the right to have private conversations, to send private messages, and to keep private files — and we do have that right today.

Encryption is not yet in widespread popular use, but it should be soon. Telephone users are becoming increasingly annoyed with the fact that nosy people can easily listen in on our wireless (cellular and cordless phone) conversations. As more and more people use e-mail for their correspondence, they realize that sending e-mail without encryption is like mailing a postcard — everyone can read it along the way to its destination.

But the Clinton Administration opposes our right of encryption. Vice President Al Gore, Attorney General Janet Reno, and FBI Director Louis Freeh, are all demanding the authority to read our encrypted messages. They believe that, to be sure you are not breaking the law, the Federal Government should have access to all your private files and messages at any time and without your knowledge.

That would be tantamount to giving the government the power to steam open all the letters we send through the mail. That's only done in totalitarian countries. No free nation has ever tried to snoop on the content of private messages — until the Clinton Administration.

When you put messages in code, whether it's an old-fashioned code written on paper or a newfangled code concocted on a computer, there must be a "key" to enable you and the recipients of your communications to read them. The Clinton Administration is demanding access to all encryption keys through a system called "key recovery" or "key escrow." Under one scheme, all Americans would be required to deposit the keys to their software files and communications with a "third party" who would rapidly comply with government agency requests without telling us. As an alternate, the Clinton Administration is pressuring industry to make it impossible for Americans to buy any encryption system that doesn't have key recovery built into it.

Rep. Bob Goodlatte (R-VA) says that "encryption is to digital communications what deadbolt locks are to doors." Giving the FBI access to our encryption keys would be like giving our door keys to the local police, leaving our doors unlocked, and relying on the police to catch burglars after they break and enter.

Everyone will eventually want encryption in the computer age. There are all kinds of reasons why we will want to encrypt our own computer files and e-mail and telephone calls, and also want the people with whom we do business to use strong encryption so that the personal records they have on us will not fall into unauthorized hands.

Whether you use a computer or not, enormous amounts of your personal information are already collected and stored "on line" on somebody else's computer. Doctors and hospitals store and transfer sensitive medical records. Your bank and credit card companies hold and transfer information about your finances. Your employer, and the stores where you shop, collect and transfer information about your income and purchases. The telephone company has a complete listing of every phone call you make or receive, including the phone numbers, the time, and how long you talked. The government requires cell

phone companies to track the location of your cell phone.

The Department of Health and Human Services wants to build a national computerized registry of everyone's health record and at least half the states have already built a database of medical records. HHS is also building the National Directory of New Hires with data forwarded by the states on every new worker. Of course, the Internal Revenue Service and the Social Security Administration have computer files on nearly all Americans.

The public schools are starting to participate in a national data collection system that will collect and transfer private information about all students, not only their academic records, but also medical, attitudinal, behavioral, and family information that is none of the schools' business. The plan is to have these electronic portfolios available to the government and to the students' future employers.

FBI Director Louis Freeh doesn't like Americans having private conversations. He told the Senate Committee on Commerce, Science and Transportation on July 25, 1996 that encryption poses a "threat to public safety." He wants to forbid the use of encryption products unless they are "socially-responsible," *i.e.*, have "key recovery" built into them so he can read them. He speaks ominously about what he calls "the looming specter of encryption" that he can't crack. This is the same Louis Freeh who in 1996 proposed that one percent of the telephone capacity in urban areas be reserved for wiretaps (that's 10,000 phones in a city of one million). Even the KGB and the Gestapo didn't reach that level of surveillance.

The FBI argues that it needs "key recovery" power to crack down on drug lords and terrorists, but the bad guys can buy top-quality encryption from dozens of other countries. The danger from these criminals should **not** require Americans to submit to police-state surveillance of our daily lives and activities.

The FBI cannot be trusted with the awesome power of key recovery. The FBI has already betrayed our trust in so many areas, including turning over 900 "raw" personnel files to political operatives at the Clinton White House, the multiple outrages at Waco and Ruby Ridge, and the abuse of Richard Jewell, the falsely accused Atlanta security guard.

A neutral panel of the National Research Council was set up to make policy recommendations about encryption. The panel called on the government to abandon its efforts to restrict encryption. The panel concluded that increased use of encryption would enhance our national security, not diminish it. Thirteen of its 16 members had security clearances with access to secret information, and they said there are no classified national security reasons that are relevant to the encryption debate. The Clinton Administration bases its campaign to control private encryption on the alleged need to fight crime through wiretapping, but the panel concluded that the ability of the private sector to transfer confidential financial and other data over the information highway without interception is far more important. Strong encryption for individual use is the number-one privacy issue in the information age.

Power Grab by Executive Order

The President who got by with issuing Presidential Decision Directive 25 (asserting his authority to assign U.S. troops to serve under foreign commanders) apparently now thinks he can get by with an even bigger grab for power. On May 14, Bill Clinton quietly issued Executive Order 13083 called "Federalism."

When you cut through the reassuring window dressing restating the obvious (*e.g.*, "the Constitution is premised upon a system of checks and balances"), it becomes clear that this Executive Order's real purpose is to grab large new federal executive-branch powers at the expense of the states. Clinton's Executive Order reminds us that "There should be strict adherence to constitutional principles," but (in Shakespeare's words) he "doth protest too much, methinks."

The real key to this Clinton Executive Order is that it revokes President Ronald Reagan's 1987 Executive Order 12612 on Federalism, which recognized that our Constitution reserves many important powers to the states.

Written in broad and ambiguous language, Clinton's Executive Order amounts to a bold and overreaching attempt to rewrite the U.S. Constitution, especially the Tenth Amendment. Following are some of the matters that EO 13083 asserts "justify Federal action":

- "When there is a need for uniform national standards."
- "When decentralization increases the costs of government thus imposing additional burdens on the taxpayer."
- "When states have not adequately protected individual rights and liberties."
- "When States would be reluctant to impose necessary regulations because of fears that regulated business activity will relocate to other States."
- "When placing regulatory authority at the State or local level would undermine regulatory goals because high costs or demands for specialized expertise will effectively place the regulatory matter beyond the resources of State authorities."
- "When the matter relates to Federally owned or managed property or natural resources, trust obligations, or international obligations."

Clinton's greatest skill is with words, and the words of this Executive Order were artfully chosen to sound harmless but, when interpreted by his activist judges, rationalize the exercise by the President of open-ended, ambiguous regulatory powers. If Y2K causes crucial computers to crash and precipitate a national emergency, Clinton will be ready with Executive Order 13083 to assume dictatorial powers.

Congress should immediately repudiate Clinton's impudent grab for power.

The Phyllis Schlafly Report
PO Box 618, Alton, Illinois 62002
ISSN0556-0152

Published monthly by the Eagle Trust Fund, PO Box 618, Alton, Illinois 62002. Periodicals Postage Paid at Alton, Illinois. Postmaster: Address Corrections should be sent to the Phyllis Schlafly Report, PO Box 618, Alton, Illinois 62002. Phone: (618) 462-5415.

Subscription Price: $20 per year. Extra copies available: 50¢ each; 3 copies $1; 30 copies $5; 100 copies $10.

http://www.eagleforum.org **eagle@eagleforum.org**