National Center for Policy Analysis

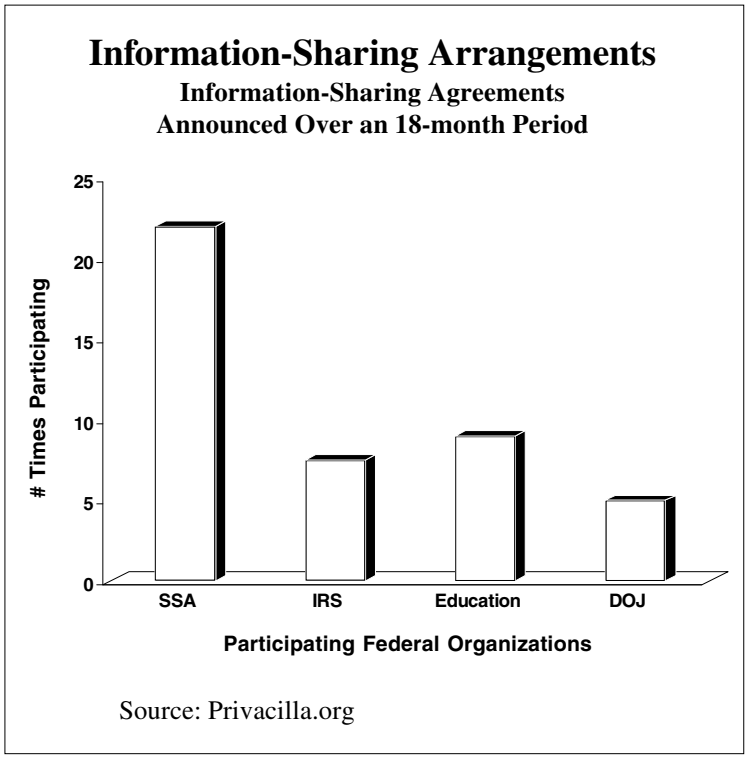
BRIEF ANALYSIS
No. 364
For immediate release:
Monday, July 30, 2001

Privacy from Government in a Transparent Society

By Devon Herrick

Individuals face a greater threat to their privacy from government than from the private sector. In general, people have little or no control over what information is collected, how much is shared or how securely it is stored. If a business refuses to keep private information about one's consumer preferences secure, consumers can take their business elsewhere. But they hardly have the same opportunity when it comes to the Department of Motor Vehicles or the Internal Revenue Service.

Government Information Collection. Government (federal, state and local) collects and shares more personal information about individuals than any other entity. A recent study by the privacy organization Privacilla found that during an 18-month period beginning in September 1999, federal agencies announced 47 times that they would exchange and merge personal information from databases about American citizens. [See the figure.]



Source: Privacilla.org

- The Social Security Administration announced involvement in 21 different information-sharing arrangements.
- The Internal Revenue Service participated in information-sharing arrangements on eight different occasions.
- The Department of Justice and the Department of Education were involved in five and nine different arrangements, respectively.
- Many of these arrangements were broad, dealing with multiple state or federal agencies.

Federal agencies routinely share information with other agencies. The Privacy Act of 1974 was supposed to protect individuals from the unauthorized use of records collected by federal agencies. Yet, agencies often violate the Privacy Act's requirement that data be collected directly from the individual rather than surreptitiously through mining another agencies' records.

Recent reports illustrate just how much the government knows about individuals:

- In order to create safe roads, states maintain information on licensed drivers including photos, physical descriptions and, sometimes, medical information. Much of this information is sold or considered public record.
- As a result of a well-meaning program to track dead-beat dads, the Department of Labor knows where you work and how long you've worked there.
- If you are on Medicare or Medicaid, the Department of Health and Human Services has information about your medical history.

Privacy Violations. Government computers are often filled with highly sensitive, very personal information. Your medical records, banking records — maybe even your life history — might be floating around government bureaucracies without your knowledge or against your wishes. The Internet raises additional questions about what information government should collect. For example, government Web sites have been known to collect information on persons who thought they were anonymously reporting information about crime. Experts worry about how closely bureaucrats follow privacy standards for what is collected and how securely information is stored.

- A study by the General Accounting Office found that 97 percent of federal government Web sites failed to meet the privacy standards (notice, choice, access, and security) recommended by the Federal Trade Commission for private sector Web sites.

Dallas Headquarters: 12655 N. Central Expy., Suite 720 • Dallas, TX 75243-1739 • 972/386-6272 • Fax 972/386-0924
Washington Office: 655 15th St. N.W., Suite 375 • Washington, DC 20005 • 202/628-6671 • Fax 202/628-6474
For more information: Sean Tuffnell in Dallas at 972/386-6272 or Joan Kirby in Washington at 202/628-6671

- These sites included the Food and Drug Administration, the Health Care Financing Administration, the Veterans Health Administration and the National Institute of Allergy and Infectious Diseases.
- A Veterans Affairs Oversight Subcommittee reported security problems within the Department of Veterans Affairs.

Nor is the threat always from the federal government. James K. Glassman, a Senior Fellow at the American Enterprise Institute, reports that the state of Florida wanted to sell drivers license data, including photos with names, addresses and vital statistics. Public outcry forced the state to abandon its plan. Not long afterward, the Florida Legislature voted to sell the state Labor Department's records (including salary information) on 6.5 million workers to consumer-reporting companies. Other states have similar programs.

Government Exemption from Privacy Protection. The new federal medical privacy regulations limit the use of medical information by private sector entities, but require doctors, hospitals and other health care providers to share patients' personal medical records with the federal government. In addition, government tends to exempt itself from regulations on information collecting. For example, the Privacy Act of 1974 has public sector exceptions. Although the Computer Matching and Privacy Protection Act of 1988 described the manner in which federal agency computer matching could be performed (adding certain protections for individuals), it had the unintended consequence of "institutionalizing" the sharing of data among federal government agencies.

Government Abuse: Rogue Employees. Even when privacy protection rules are in place, government employees can make them meaningless. At the IRS, for example:

- More than 500 employees were caught browsing through the tax records of acquaintances, friends and public figures (and only 1 percent were fired for this offense).
- A former official historian for the IRS reported that the agency once compiled its own "enemies list" of 11,000 Americans who criticized government policies.

Abuses occur at other levels of government, too. For example, in 1994, medical records department employees at Parkland Memorial Hospital, a county-operated hospital in Dallas, were accused of selling medical information on patients to outsiders who could profit from its use.

Government Abuse: Threats to Human Rights. The classic example is the use of U.S. Census data at the outset of World War II to identify citizens of Japanese ancestry to be rounded up and placed in internment camps. There is also a danger that authorities, using a technique called data mining, might identify *seemingly* unrelated traits often associated with criminal activities and use these to target people never accused of a crime. Similarly, demographic data might be used to target neighborhoods for racial profiling.

Government Abuse: Excessive Enforcement. Less understood is how information may be gathered today and used in the future to allow overzealous enforcement of laws. Many laws are often (at least partially) ignored because society only supports a certain level of enforcement. For example, drivers routinely exceed the speed limit slightly, yet most people expect only the most flagrant violators to be cited. Yet global positioning satellite technology makes it possible to track all speed limit violations. Likewise, most people don't expect teenagers to report low-level earnings to the IRS for occasional baby-sitting or lawn mowing services, but soon it will be easy to record all personal service transactions and match them with spending habits.

Government Abuse: Coercion. The Fourth Amendment to the Constitution protects us from unreasonable search and seizure, and the Fifth Amendment protects us from incriminating ourselves. However, both protections are under threat if authorities can surreptitiously gain access to databases of information with personal profiles from health care providers, bankers and retailers, or if officials use technology that passively discovers information about individuals without their knowledge.

Conclusion. Although some degree of information sharing is undoubtedly beneficial, information in the hands of government can pose a threat to individual rights. Individuals have less recourse to a remedy when government inappropriately invades their privacy than when the offender is a business or another individual. If Congress wants to expand or enhance privacy protections, the best place to start is with the government's own information collection and sharing policies.

Devon Herrick is Research Manager for the National Center for Policy Analysis.