the Selective Service bought the birthday list from a major ice cream parlor chain that gave free sundaes to customers on their birthdays. The list was used to find 18-year-old men who had not registered for the draft.\(^{16}\) The FBI proposed expanding NCIC to include access to many large private and government databases, including those maintained by credit bureaus, insurance companies, telephone companies, airlines, banks, the IRS, the Social Security Administration, and the Immigration and Naturalization Service (INS). The plan was scaled back because of opposition from people concerned with the potential for privacy and civil-liberties violations, but in 1996, Congress authorized millions of dollars to expand NCIC and link it to more databases.

Many government agencies, including the IRS, the FBI, and the INS, quietly found a way to access huge amounts of personal data not in their own databases: They buy personal information from private information service companies. Thus they “outsource” collection of information it would be controversial and possibly illegal for them to collect themselves. One private firm, ChoicePoint, for example, culls data from the three big credit bureaus, numerous local, state, and federal government agencies, telephone records, liens, deeds, and many other sources. ChoicePoint bought more than a dozen other personal information companies whose databases included records on drug tests, doctors’ backgrounds, insurance fraud, and other areas. In 2001, the firm had more than 10 billion records in its system. ChoicePoint’s clients include at least 35 government agencies. It has multimillion-dollar contracts with the Justice Department and the IRS and maintains a Web site for the use of FBI agents.* The writers of the Privacy Act and government data policies did not anticipate and explicitly cover the huge amount of information the government can buy from private information services. Some observers, including a former chief prosecutor in the Justice Department’s computer crime unit, say that, if the government is not allowed to collect certain data, then it should not be allowed to buy it. The FBI and the INS argue that they are simply using a new tool to collect information and evidence they used to collect themselves before, but much less efficiently.\(^{17}\)

As part of its efforts to enforce drug laws, the federal government maintains a database of people who have legally bought certain prescription medications (e.g., pain relievers containing narcotics). Does the potential value of the database in a criminal investigation justify the invasion of privacy of the vast majority of people using the medication appropriately?

**BURDEN OF PROOF AND “FISHING EXPEDITIONS”**

As some of our examples illustrate, computer technologies have altered the nature of tax, criminal, and other government investigations. Law-enforcement agencies obviously need to collect evidence from a large variety of sources. Traditionally, law-enforcement officials started with a crime and used a variety of techniques to look for a suspect. Now

---

*ChoicePoint won a “Big Brother” Award at the annual Computers, Freedom, and Privacy conference. The award is given to businesses and government agencies whose practices are particularly offensive to privacy advocates. The company was fined $1.37 million by the state of Pennsylvania for selling driver data in breach of a contract with the state for processing driving records.