IDEAS ON LIBERTY
MAY 2003

The State's Quest for Total Information Awareness

by David M. Brown

Efforts to transform the United States into a surveillance regime on a totalitarian or quasi-totalitarian model are currently underway.

In addition to attempts to beef up and make uniform the state driver's licenses—thereby blending them into either a de facto national ID card or the immediate precursor to one—attempts are also in progress to impose a "trusted traveler card" on all air passengers. This card could also be the precursor to a mandatory national ID card designed to help the government monitor your movements. The most ambitious plan yet to electronically canvass Americans, however, is the Defense Department's Total Information Awareness (TIA) project. The goal is to rummage through the private transaction records of everyone in America, including people who never leave the house.

Congress has put restrictions on the development of TIA but so far it has not eliminated the program. Therefore, it is premature to regard the issue as dead.

In "The Pentagon Ramps up the War on Privacy" (*Ideas on Liberty,* April), I pointed out that at the very least, the TIA database, if built, would be susceptible to all the errors and crimes to which all other databases are susceptible—with the added advantage of hyper-centralization of our recorded transaction data so that a vindictive clerk or random hacker need only violate a person's privacy once in order to wreak havoc across the board. I presented some of the history of private databases. Perhaps you will not be surprised to learn that governmental databases are no less subject to blunders and breaches of security.

"[E]rror rates for Internal Revenue Service data and programs are typically in the range of 10 to 20 percent," report Cato Institute authors John J. Miller and Stephen Moore. "A 1989 General Accounting Office study determined that 20 percent of a sample of INS data on aliens was incomplete and 11 percent of the files contained erroneous information. The National Law Journal reported . . . that INS files on 50,000 Salvadoran and Guatemalan aliens 'routinely contained the first and last names in the wrong order.' It also discovered that 'a name search was impossible because data was repeatedly entered into the wrong data field, that misspellings were rampant, and that numbers were often used in place of letters.' Even Social Security files have been found to contain error rates in 5 to 20 percent of cases."[1] There is no reason to think that any centralized database forming the hub of a surveillance regime would be immune to such errors.

Bad policy is another problem. While there are no statistical measures of bureaucratic lapses in judgment, there is plenty of anecdotal evidence. One example occurred in 1997, when taxpayers learned that the

---

David Brown is a freelance writer and editor. This is the second of two parts.

Social Security Administration (SSA) was providing tax data about individual taxpayers over the Internet. The SSA argued that because taxpayers would be obliged to enter their name, date and state of birth, and mother's maiden name before they could download their private information, their information would be secure. While such "security" may have been good enough for government work, the flak from taxpayers (plus the prospect of a Senate investigation) persuaded the agency to amend the system.[2]

The Securities and Exchange Commission (SEC) is another security naïf. Until mid-1997, the SEC routinely collected Social Security numbers (SSNs) on filings that were then made available on its website. It had to revise its procedures to accommodate privacy concerns. "With the growth of the EDGAR database, and its availability to millions of viewers on the commission's Web site, the commission is concerned that these numbers are too readily available," said the SEC in explaining the rule change. "The usefulness of Social Security numbers filers voluntarily provide on these forms is outweighed by the risk of misuse created by the disclosure of those numbers." Yet a few years later the SEC had yet to remove or modify older documents on the site that still displayed SSNs. The SEC would not even black out the numbers on the screen. SEC spokesman John Heine told reporters, "We can't alter those forms. They are a matter of public record."[3]

Nonchalance with Records

In his book *A Law Unto Itself*, David Burnham notes that one of the areas in which the Internal Revenue Service has demonstrated "considerable nonchalance is in its protection of the confidential information it collects on the financial, medical, and other personal secrets of every taxpayer." This is despite the fact that the Tax Reform Act of 1976 "sets a high legal standard for the IRS: Personal tax return information is not to be disclosed to any other organization or person except in certain precisely defined situations. The law made it a crime for any IRS employee to violate these rules."[4]

Burnham found that, as late as 1989 (when his book was published) it was all too easy to tap into the IRS's computers—though, until then, there had been only one reported instance of a hacker's doing so. A greater risk for taxpayers is that an employee entitled to access the data will do so for personal reasons. Despite recurring instances of illicit "browsing," until recently agents caught doing this could not be prosecuted unless they had also revealed the information to others. In 1997 the First Court of Appeals dismissed a case against an IRS agent on those grounds.[5] Partly as a result, Congress tightened the law. Even if invasive browsing is technically prohibited, however, there is not much a victim can do unless he first knows that it is going on. The deck is somewhat stacked against victims of the government anyway. IRS personnel, like those of other high-power federal agencies, often feel free to act above the law; and even when chastised for doing so, they often get little more than a slap on the wrist.

Sometimes bureaucrats are more than nosy or careless; sometimes they are outright criminal. In 1996 the government accused a gang of clerks at the Social Security Administration of appropriating the data of more than 11,000 people. The clerks had sold the information to crooks, who used it to activate stolen credit cards. The legitimate cardholders soon found themselves encumbered with huge unexpected bills.[6]

Policemen and others in law enforcement have also pilfered databases—in pursuit of personal, political, and criminal ends. In quest of a girlfriend, an Australian policeman performed thousands of unofficial searches of a police database. He later claimed that many of the searches were "training exercises."[7] Police in Highland, Indiana, were excluded from an FBI database after officers were accused of repeatedly abusing their access.[8] The Shawnee County, Kansas, sheriff's department was investigated for running criminal background checks on organizers of a campaign to recall the sheriff.[9] A sheriff's lieutenant in Mary-

land was charged with plundering a database to help out local Democrats.[10] A former FBI agent teamed up with a worker in the Nevada attorney general's office to sell information from the FBI's database to the mob.[11] A Detroit police officer tapped into the Law Enforcement Information Network and other police databases to investigate his wife and her acquaintances; he was later suspected of complicity in her murder.[12]

There are many other cases.

Public-Private Cooperation

When confidential data isn't being scavenged by rogue employees, it may be given or sold by management itself. Government agencies sell personal information to private firms and vice versa, usually without the knowledge and permission of the persons involved. For example, Maryland state employees sold private information on Medicaid recipients, including their Social Security numbers, to HMOs seeking new customers.[13] Some such abuses may be illicit, but others are just standard operating procedure.

Cash-strapped state governments will sell driver's-license data if they can. In 1999 the New Hampshire firm Image Data was negotiating to buy the driver's-license databases of five states, and planned to acquire the databases of all the states, until public objections killed the effort, at least temporarily. South Carolina Attorney General Charlie Condon filed a lawsuit to prevent the federal law that authorized the sale of private driver's license information from going into effect.[14] It turned out that Image Data was funded largely by the federal government, and that the Secret Service was involved in the development.[15] The goal was to create a national database of driver information and photos that would be at the disposal of the federal government, as well as perhaps retailers cashing checks.[16] According to Image Data, its intention was to prevent fraud and tighten privacy safeguards.[17]

Money is not always an incentive. In the wake of 9/11, many private organizations have been eager to hand over entire databases to the government to help in the fight against terror. For example, based on mere vague threats of an attack that might involve skin-diving terrorists, the Professional Association of Diving Instructors (PADI) gave its entire membership database to law enforcement—even though it had not yet been obliged to do so by court order, subpoena, or other legal compulsion.[18] Any prior respect for the privacy of its members was apparently now moot. Over the past year and a half, vague terrorist threats have encompassed virtually every aspect of America, from trains to apartment houses. According to the reasoning followed by the officers of PADI, no firm or organization whatever could be justified in declining a polite request from the government to inspect the private information of its customers or members.

And once government gets our information, it is all too liberal about redistributing it. Devon Herrick, a researcher with the National Center for Policy Analysis, notes that people "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 (federal, state and local) collects and shares more personal information about individuals than any other entity." Herrick pointed out that 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."[19]

The conduct of both private and governmental entities suggests that, even if the data-scavenging regime imagined by Poindexter did somehow nip in the bud the bomb-throwing breed of terrorism, it would also increase everyone's vulnerability to cyber-blundering, cyber-crime, and cyber-

terrorism. The privacy-violating character of the government's reporting requirements for private transactions (such as for all bank transactions of $10,000 or more), though egregious, has until now been mitigated by the fact that the information collected is not generally available except to the clerks shuffling the data, investigators pursuing a specific case, bureaucrats pursuing a vendetta, and possibly hackers. Under the TIA regime, all that would change. Not only would the centralized depository required by such a regime present a more inviting cyber-target than ever; the costs paid by the victims of successful hacks would be greater than ever as well. And how hard would it be, really, for a determined cyber-terrorist to get a job as a clerk where he could do a lot of damage? It's not as if you'd need only three or four people to maintain the TIA database.

Brave New World

The creators of Total Information Awareness claim that if their dream is realized, privacy would be respected and security protocols would be ironclad. But no database, regardless of purpose or public assurances, can be entirely secure from careless or unscrupulous persons. Even the most robust security system is susceptible to an inside job—or to typos. No matter how heavily armored, no functioning database can be entirely sealed off from intrusion. The reason is that *every database must be capable of being read and updated*. Someone is doing the reading; someone is doing the updating. Many of these people are ordinary clerks.

In the best of all possible national-identification regimes, the people entering and safeguarding our data would be invariably careful, sensible, and honest, never violating the implicit trust in them. But we know that this is not the case. It might be reasonable to expect a high level of trust when requested information is specific to a given transaction, provided voluntarily, and safeguarded by persons who can be held accountable. But the many and growing documented cases of abuse by those entrusted with our data, especially when that information is grabbed and transferred by force, show that this is not a reasonable expectation. Even supposing the TIA protocols to be more "secure" than what the Social Security Administration or motor vehicle departments consider to be "secure," it will still be the case that the persons whose privacy and security are at stake would not be allowed any choice in the matter. Robbing the individual of his freedom to make those decisions himself—decisions about who gets his private information and under what circumstances—can only render his private affairs less secure and more vulnerable.

Of course, in the new surveillance regime, the problems caused by errors, dishonesty, or lack of accountability would only be exacerbated for those saddled with the "wrong" national or ethnic background, or with the unfortunate necessity of having to conduct "unusual," flag-raising bank transactions.

In April 2002 almost half of a group of protesters on their way to Washington, D.C., were forced to miss their flight because their names were similar to names on a watch list. One of the passengers was named "Jacob Laden."[20] There could be lots of trouble for certain people if a radical Islamic terrorist ever decides to go by the name of "John Smith." These incidents are frequent enough as it is. Imagine how many more opportunities there would be for "profile matches" if, down the road, airport security personnel were able to check your ID against all the varied information collected on you in the Total Information Awareness database.

We will not increase our personal security by making it easier and easier for more and more strangers to roam through our private records. Given the potential for abuse, it would be better if as little personal data as possible were collected, tailored always to the specific purposes of a transaction. Such data as is collected should be treated as a sacred trust. To decrease the likelihood and costs of cyber-invasion, the security of existing databases should be fortified when necessary. But except when criminal records are involved, databases that are now segregated

from each other must remain segregated. Yet projects like the updated Computer-Assisted Passenger Prescreening System (CAPPS II) or Total Information Awareness would send us hurtling in the opposite direction, integrating all kinds of disparate, innocent private data about us into a single centralized database, in blatant violation of our rights. By treating everybody as a suspect, such overreaching would turn everybody into a potential victim. And not on a temporary wartime "emergency" basis, either. Once such databases are created, they don't fade away. They just get copied and recopied.

Total Disinformation

Some have suggested that if the Total Information Awareness program fails to achieve its utopian goal of omniscience about the motives underlying a citizen's transactions, it would pose little actual danger to our privacy.

In fact, only if the recommended database is never built or used at all could there be no danger to us. We must not forget that many in government have hoped to create a centralized, comprehensive national database about all Americans and resident aliens at least since the 1960s. These demands have grown more insistent. National employment databases, national medical databases, national criminal databases, and others have already been created. The dream is to blend all these separate resources into a single centralized one. The existence of a now-universal data tag like the Social Security number has made it possible to collate and retrieve all this information in a single scoop, without complicated algorithms or sophisticated artificial intelligence. Certainly the data storage problem has been solved; computer memory grows cheaper and more powerful every year. Whether or not the desired data-mining software can be programmed, the only real impediments to creating the database that now remain are political and cultural: the stubborn assumption of so many Americans that they have rights.

Now is the time to appeal to that independent spirit. Sooner or later, the database would be used for many other purposes besides second-guessing terrorists—who, one must assume, would do their best to avoid fitting the profile (and who need accomplish their goals only once in any case). A national ID card—the final nail in the coffin of our right to roam unhindered as free men and women—would be a natural next step. Once a centralized database of all our transactions is built, it will be that much easier to impose such a card—even if those who authorize and erect the database promise that it will never be used for that purpose. Even if such promises are made in good faith, the people shaping policy today will not be shaping policy tomorrow.

The complex data-mining that Poindexter wants to install is a massive endeavor that will take years of arduous work to accomplish, if it can be accomplished at all. Implementation will require additional authorization from Congress. But we can hardly be optimistic that the legislators will suddenly "see the light" if they fail to quash the project before TIA becomes operational. CAPPS II is similarly intrusive, and much closer to launch date; meanwhile, its predecessor has been in use for years. The principle of such intrusive data-canvassing is thus already widely accepted. Certainly, notwithstanding periodic controversies about the privacy issues involved, congressmen have allowed many of the intrusions to persist. Indeed, they have often inaugurated them.

Before the Homeland Security Act was passed last fall, some feared that it would authorize not only the funding of TIA development—already being funded anyway to the tune of hundreds of millions of dollars over the next three years—but also its ultimate implementation. Getting TIA on line would require the power to order all banks, phone companies, credit-card companies, Internet service providers, and the like to hand over all their records, without ever being served with legal papers. Such authority might well have been explicitly stipulated in the Act had not *New York Times* columnist William Safire and others spread the alarm prior to the bill's final passage.

Last year former representative and majority leader Dick Armey stressed that the Act "does not authorize, fund or move into the [homeland security] department anything like [TIA]"; and that the use of data-mining tools in the bill are "intended solely to authorize the use of advanced techniques to sift through existing intelligence data, not to open a new method of intruding lawful, everyday transactions of American citizens."[21]

Armey's characterization of the Homeland Security Act may be technically correct. But we know that some of the required authority already exists de facto (for example, insofar as banks are required to report certain kinds of financial transactions of their customers to the government, employers are required to report on their new employees to help build a national employee database, and so on). And the Homeland Security Act as passed provides for a "Directorate for Information Analysis and Infrastructure Protection," which would be empowered to "access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies, *and private sector entities*, and to integrate such information in order to . . . detect and identify threats of terrorism against the United States."[22]

What this broad mandate will mean when it comes to seizing private data remains to be seen. It is true that eventual congressional authorization (whether tacit or explicit) of a ready-to-roll TIA program is not inevitable. But it is hard to see what principled objection the national lawmakers could raise in light of the precedents they have already sanctioned. If Total Information Awareness is to be stopped, it will most likely be stopped not by the principles or natural inclinations of politicians, but by the principles and protests of constituents. □

1. John J. Miller and Stephen Moore, "A National ID System: Big Brother's Solution to Illegal Immigration," Cato Institute Policy Analysis no. 237, September 7, 1995, www.cato.org/pubs/pas/pa237.html.

2. Ibid., p.10.

3. Courtney Macavinta, "SEC still listing Social Security IDs," CNET News.com, March 23, 1999.

4. David Burnham, *A Law Unto Itself* (New York: Random House, 1989), pp. 124–25.

5. *United States v. Richard W. Czubinski*, February 21, 1997, www.law.emory.edu/1circuit/feb97/96-1317.01a.html.

6. Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol, Cal.: O'Reilly & Associates, 2001), p. 30.

7. John Taylor, "Constable admits using police database for personal reasons," Australian Broadcasting Corporation, March 2, 2000, www.abc.net.au/am/s105272.htm.

8. "Local PD Shut Out of Indiana Crime Files," *Law Enforcement News,* November 15, 2000, www.lib.jjay.cuny.edu/len/2000/11.15/index.html#access.

9. Steve Fry and Kevin Bates, "Misuse of Background Checks Alleged," *Topeka Capital-Journal*, April 4, 1999, http://cjonline.com/webindepth/meneley/stories/040799-2_meneley.shtml.

10. Annie Gowen, "Lieutenant Faces More Charges; Sheriff's Probe of Records Misuse Alleges 102 Violations," *Washington Post,* April 20, 2000.

11. Jeff German, "FBI-leaks investigation widens," *Las Vegas Sun*, August 28, 2001, www.lasvegassun.com/sunbin/stories/sun/2001/aug/28/512276279.html.

12. M. L. Elrick, "Police say suspended cop abused database," *Detroit Free Press*, August 8, 2001, www.freep.com/news/mich/lein8_20010808.htm.

13. Charles Sykes, *The End of Privacy: The Attack on Personal Rights—at Home, at Work, On-Line, and in Court* (New York: St. Martin's Press, 1999), p. 26.

14. "States Sell Drivers' Digital Photos," Network USA, www.networkusa.org/fingerprint/page1b/fp-dl-photos-top-page.html.

15. Claire Wolfe, "Little Brother Is Watching: The Menace of Corporate America," *Loompanics Unlimited*, Winter 1999, www.loompanics.com/Articles/LittleBrother.html.

16. Declan McCullagh, "Smile for the US Secret Service," *Wired News*, September 9, 1999, www.wired.com/news/politics/0,1283,21607,00.html.

17. "Identity Crime Prevention Pilot Program Digitization Process Development Justification," Image Data, LLC. Archived by Electronic Privacy Information Center at www.epic.org/privacy/imagedata/image_data.html. See also Robert O'Harrow, Jr., and Liz Leyden, "U.S. Helped Fund Photo Database of Driver IDs; Firm's Plan Seen as Way to Fight Identity Crimes," *Washington Post*, February 18, 1999.

18. See Jeff Elkins, "Playing PADI Cake With Liberty," June 13, 2002, www.elkins.org/modules.php?name=News&file=article&sid=306. See also "FBI Investigating Florida Dive Shops," nbc6.net, June 3, 2002, www.nbc6.net/news/1493244/detail.html.

19. Devon Herrick, "Privacy from Government in a Transparent Society," Brief Analysis No. 364, National Center for Policy Analysis, July 30, 2001, www.ncpa.org/pub/ba/ba364/. See also "Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information is Systematic and Routine," Privacilla.org, March 2001, www.privacilla.org/releases/Government_Data_Merger.html.

20. Gena Kittner, "3 USWP students detained at airport," I, *Wausau Daily Herald,* April 24, 2002, www.wausaudailyherald.com/wdhlocal/275083752718269.shtml.

21. Dick Armey, "Homeland Security Protects Privacy," *Congressional Record,* November 22, 2002.

22. See "An Act to establish the Department of Homeland Security, and for other purposes [H.R. 50005]," Title II—Information Analysis and Infrastructure Protection, Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information; archived by FindLaw, http://news.corporate.findlaw.com/hdocs/docs/terrorism/hsa2002.pdf; emphasis added.