IDEAS ON LIBERTY
APRIL 2003

The Pentagon Ramps Up the War on Privacy

by David M. Brown

[**Editor's Note:** *As we went to press the U.S. Congress had hampered the Defense Department's ability to carry out the threat to privacy discussed in the following article. Under the provision adopted the Pentagon cannot proceed until it assesses for Congress the effects on civil liberties and cannot target American citizens without congressional permission. Unfortunately, the provision does not kill the program outright, but only, in columnist William Safire's words, puts "a bit in the mouth of the Pentagon's runaway horse."*]

In May 1997—several years before the terrorist attacks in New York City and Washington, D.C., "changed everything"—Charles Simonyi got a glimpse of the future. He fit the profile, and he was targeted.

Simonyi, a Hungarian-born computer engineer employed by Microsoft, had been through the drill many times before. He knew that the airport security people sometimes inspect carry-ons, and he was prepared for that. He knew that pocket change could set off the metal detector, and he was prepared for that, too: no pocket change. He knew that getting through security would go more smoothly if he was pleasant and compliant, so he was prepared to be pleasant and compliant. One thing he could not know, however, was how to make sure he would never "fit the profile" of a potential terrorist. And he did not know how to remain unruffled when singled out for humiliating attention—as the computer had singled him out this Friday.

> With no lines at security, I got through in record time. My bags got X-rayed, and my level of whatever those portals you walk through measure was determined to be under the threshold. . . . A supervisor appeared . . . and handed me to Junior, who then proceeded—methodically, if not neatly—to unpack everything I was carrying, and to toss my clothes, toiletries, etc., into a dirty bin nearby.
>
> Then it hit me. It was not that security was especially tight: It was only me they wanted. And that 'May I?' polite foreplay had gone out the window. The label my friendly hometown airline had affixed to my bags had unexpectedly made me a marked man, someone selected for some unknown special treatment. The routine was broken; the power had shifted; the violation had begun. I suddenly felt as if in the grip of a giant vise, a terrible feeling I had last experienced as a teen-ager before fleeing Communist Hungary.
>
> When I recount this story to friends, this is where they start to smile, as if a diagnosis of my condition had suddenly become apparent. After all, if someone with post-traumatic stress disorder jumped two feet

David Brown (dmb1000@juno.com) is a freelance writer and editor. This is the first of two parts.

A major step in imposing a national identification regime would be the establishment of a centralized computer database to which a prospective ID card could be linked.

> in the air every time a door slammed shut, good friends would be more concerned about the person's condition, not the door. In a like manner, my friends may suspect I am suffering from some Hungarian Refugee Syndrome, which makes me overly sensitive to perfectly reasonable intrusions by the state.
>
> I try to explain: The communism I had fled was hardly traumatic or violent. One aspect of the horrible vise was the constant minor humiliations I had to suffer, such as interaction with the block warden, the party overlord of a block of houses, who had to give his assent to all matters tiny or grand, including travel. On this Friday in the United States, I was being singled out for an unusual and humiliating search. My personal goal was to fly to Los Angeles for a meeting that was important to me. If I had refused the search—cried 'NO!' as it were—I assume they would have let me go home, but I would have been forbidden to board the plane and would have missed my meeting. So I did what I had done 30 years ago: I chose to be humiliated just so I could reach my goal.[1]

From a form letter, Simonyi learned that passengers were being targeted for special treatment "both randomly and through an objective systematic approach based on direction from the FAA." He was witnessing something new in America. The federal requirement that air passengers present IDs in order to board domestic flights had been imposed just a year earlier. By the end of 1997, passengers were being routinely scrutinized by something called the Computer-Assisted Passenger Prescreening System (CAPPS I), a form of data-mining implemented by the Federal Aviation Administration that is supposed to peg which passengers are most likely to be terrorists. CAPPS does not necessarily finger people based on any *actual* evidence of either past or planned wrongdoing. Yet as Simonyi's experience makes clear, in America's burgeoning surveillance regime one may be treated like a criminal suspect just the same—guilty until proven innocent. All that is necessary is that one "fit the profile"—however that profile may be defined. CAPPS may not yet have been in place when he was treated like a criminal suspect in the spring of 1997. But the animating principle was certainly in place.

Total Information Awareness

Charles Simyoni's experience shows what Americans can expect on a routine basis—and already are beginning to see, in airports—if the surveillance regime now being planned for this country is ever fully instituted. Most people would not have to endure arrest or imprisonment, only continuous harassment and humiliation, including regular inspection of private data that they would never otherwise reveal to strangers. Some of us would learn to regard such treatment as "normal" and as "the price we must pay" for our freedom, or what's left of it by then. Others would never get used to such treatment—never regard it as reasonable to be treated like a criminal suspect when they have not done anything wrong.

In a previous article for *Ideas on Liberty*, I noted that after the terrorist attacks in New York and Washington, calls for a national ID card grew more frequent and insistent.[2] I added that in a still relatively free country like the United States, a full-fledged national

The kinds of data that would be collected for analysis include educational, travel, medical, veterinary, country entry, transportation, housing, government, "critical resources," and communications (presumably including telephone records and web-surf records).

identification regime is unlikely to be imposed in a single wholesale reform. Rather, it would be imposed in incremental, precedent-setting stages. Once the invasive infrastructure was fully in place and woven into the web of everyday routine, it would be difficult to reverse the new "security" rituals. Even if the threat of global terrorism were to fade, what Milton and Rose Friedman call "the tyranny of the status quo" would likely prevail.[3] And in any case, there would always be criminals and mad bombers out there somewhere to provide a rationale for almost any level of surveillance. Such a sweeping forfeiture of rights to privacy and freedom is no temporary emergency measure that may be easily dismantled "once the war is over."

A major step in imposing a national identification regime would be the establishment of a centralized computer database to which a prospective ID card could be linked. In one respect the most zealous advocates of national identification are more ambitious than any pre-computer totalitarian state ever was. They not only want to compel the cardholder to establish "proof" of his identity at specific checkpoints. They also want to track and monitor the cardholder's movements and electronic transactions—with the records warehoused in a convenient enough form that bureaucrats and security personnel would not have to rummage through separate depositories of information to perform each investigation.

The proposal to combine state driver's licenses into a de facto national ID, linked to a national database, is one front on which this battle is being fought. Another is a proposal to issue a "trusted traveler" card to air travelers. Carol Hallet, president of the Air Transport Association of America, believes that airport security should have the capacity to tap the full range of government databases—from arrest records to immigration files and customs files. Reportedly, the federal government is indeed planning to establish a computer network that would hitch reservation systems to an array of private and government databases. The Transportation Security Administration is struggling to expand the Computer-Assisted Passenger Prescreening System into a far more comprehensive and extensive program, CAPPS II. All the private data CAPPS II taps would be analyzed with "data-mining and predictive software to profile passenger activity and intuit obscure clues about potential threats, even before the scheduled day of flight." Patterns of activity would generate a mind-reading "threat index," and passengers with a too-high index would be obliged to endure further scrutiny.[4]

All this is the backdrop to yet another effort to electronically canvass Americans, and the most ambitious one thus far: the Defense Department's Total Information Awareness (TIA) project, a project proposed and led by Vice Admiral John Poindexter of Iran-Contra fame. If built, this electronic dragnet would rummage through the private records of everyone, including people who never leave the house. In Poindexter's words, TIA's goal is to "break down the stovepipes" that currently separate private and public databases.[5] An astonishing range of electronically recorded personal-transaction data would be grabbed—with-

A dishonest clerk at the Social Security Administration could not gain a fast track to your checking account or credit-card account if neither were flagged with your SSN, as is legally required.

out permission, without subpoena, without warrant, without a side glance at the Fourth Amendment of the Constitution—and thrown into a single mammoth, computerized cauldron.

Although at least one defender of TIA claims that the project has value at least as a research project that would, allegedly, help the military or intelligence agencies defend us against the cyber-assaults of America's enemies,[6] its crafters have not been coy about the program's actual goal: to sweep aside previous restrictions on indiscriminate spying on Americans and their doings. "We must become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options," Poindexter says.[7]

The Information Awareness Office declares openly its aim of "revolutioniz[ing] the ability of the United States to detect, classify and identify foreign terrorists—and decipher their plans—and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts. To that end, the TIA program objective is to create a counter-terrorism information system that: (1) increases information coverage by an order of magnitude, and affords easy future scaling; (2) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; (3) can automatically queue [sic] analysts based on partial pattern matches and has patterns that cover 90 percent of all previously known foreign terrorist attacks. . . ."[8]

The kinds of data that would be collected for analysis include educational, travel, medical, veterinary, country entry, transportation, housing, government, "critical resources," and communications (presumably including telephone records and web-surf records).[9]

Are there risks to such data scavenging? Even for innocent people?

The Dangers of Databases

Such super-snooping is not without precedent. We do have a track record to consult . . . and the track record is not auspicious. The hazards of coercive data collection are myriad and have become more severe and obvious as private data has become easier and easier to collect, store, and retrieve—all without the permission and often without even the knowledge of the persons whose information is being pilfered. Any pledges of confidentiality that attend the construction of TIA-style data scooping must be considered in light of similar promises in the past, promises that have often been broken.

Once your personal information is typed into a database, linked and tagged by such "identifiers" as the now-all-important Social Security number (SSN; originally mandated by government, of course), that is not the end of the matter. Your private information is not only stored, it is used; and not merely for originally stipulated purposes. Government agencies that acquire private information have indeed readily divulged that data to other government agencies—and sold it to private companies. In turn, private companies have often sold private information to other private companies and to the government. Meanwhile, thieves bribe and steal from both.

Vendors and credit-card agencies are certainly culpable when they release highly sensitive information without the permission of the owners. Such actions are tantamount to leaving a customer's safety-deposit keys right out on the table for anybody to grab. But many now-commonplace abuses of privacy would never have been possible to begin with had the government never ordered that so much of our private data be linked and labeled by a single numeric key that is knowable to anyone who has a name, a valid recent address, and $50 to pay a website. Yet in the arena of personal privacy, as in many other arenas, advocates of government intervention often find it convenient to ignore the destructive consequences of previous government intervention along the same lines.

In recent years, thanks in part to the accelerating ease of electronic-information distribution, incidents of credit-card fraud and identity theft have skyrocketed. Though exact numbers are unavailable, guesstimates range from "between 500,000 and 750,000 separate cases of identity theft in 2000" alone. "Identity theft has become such a common crime," notes privacy expert Simson Garfinkel, "that individual cases no longer warrant newspaper coverage: what garners coverage now are identity theft rings—groups of criminals who steal the names, SSNs, and credit histories of dozens or hundreds of people at the same time. Identity theft rings have been found operating out of the Social Security Administration, the human resources departments of Silicon Valley startups, and even multinational telephone companies."[10]

Although abetted by computerization, much of the vulnerability here is attributable at root to the government mandate. After all, a dishonest clerk at the Social Security Administration could not gain a fast track to your checking account or credit-card account if neither were flagged with your SSN, as is legally required. The clerk might still be able to rob you if he had enough other information to work with. But without a single and ubiquitous data-tag like the SSN, it would be harder.

Private Abuse of Private Data

Criminal activity may be facilitated by firms that are careless about the hazards to which they expose their customers. For example, in 1996 Lexis-Nexis—which makes a large amount of personal data on individuals available to its customers—went so far as to publish the SSNs of almost all residents of the United States in its P-TRAK database. The ensuing uproar implied that many citizens understood a fact of life that had somehow eluded the folks at Lexis-Nexis: that the SSN had become both a near-universal identifier and an almost totally insecure one, much more dangerous to hand out to strangers than a home phone number. Swamped by angry callers, Lexis-Nexis shut down their new "service" less than two weeks after introducing it.[11]

Yet this firm's lapse in judgment consisted only in making even more easily available the kind of information that is already easily available. Even under the minimal safeguards to which the credit-card reporting firms are subjected—and which they chafe under[12]—it is easy enough to assume the role of a vendor, employer, or landlord who is "entitled" to view a consumer's credit-card history. While the reporting firms are not the most responsible culprit in all this, critics are right to suggest that these firms could do a lot more than they do to prevent credit-card fraud and identity theft.[13]

When the credit-reporting firms are not giving your information away without your permission, they are losing it to crooks, sometimes in great gobs, as customers of Ford Motor Credit recently discovered. In May 2002 Ford reported that someone had stolen the firm's access code for 13,000 credit files maintained by Experian, one of the "three big" credit-reporting firms. The perpetrators downloaded "everything they needed to assume a person's identity and open a credit card or bank account in his or her name. Experts say the thieves could also establish telephone or utility service in the person's name, obtain a loan, or use the information to obtain government documents or even government benefits."[14] Ford and its customers were not the only ones who had to worry about the rip-off. Only 400 of the 13,000 files downloaded using the company's access code belonged to patrons of Ford Motor Credit.

Large-scale cyber-snatching of privileged information grows ever more prevalent. Sometimes it looks like the kind of thing a terrorist might do. In January 2000 a hacker boasted that he had swiped 350,000 names and credit-card numbers from the website of CD Universe, a music store. He demanded $100,000 for the return of the information. To demonstrate his sincerity, he posted the information of several thousand customers on the web. SalesGate.com and the Western Union website have also been victimized by cyber-snatchers. In September 2000 Western Union reported that a hacker had grabbed the credit-card information of 15,700 customers.[15]

Sometimes the crooks work for the company. In March 2002 a former employee of the Prudential Insurance Company was arrested for stealing information from a 60,000-name database, then distributing it over the Internet.[16] The employee, Matthew McNeese, posted messages selling or even giving away the names, the Social Security numbers, and the credit-card numbers of his victims.

And it's not just the bad guys who are mauling our data. Innocent errors by bored data-entry clerks can also wreak havoc. In 1991 an investigator for Consolidated Information Service, a mortgage reporting firm, found after examining 1,500 credit reports from the "big three" that 43 percent contained errors. In the same year, 1,400 homeowners got a bad rap when a TRW contractor mistakenly characterized tax bills as tax liens. It was not easy for the homeowners to get their credit reports corrected. A similar snafu occurred a year later in Cambridge, Massachusetts; this time it was an Equifax contractor who screwed up.[17]

What about government databases? Are they immune to the kinds of hazards and glitches that have afflicted private data collection? We'll review some of the track record in that arena next month. □

[1] Charles Simonyi, "I Fit the Profile," Slate.com, May 25, 1997, http://slate.msn.com/default.aspx?id=2058.

[2] David M. Brown, "The Danger of National Identification," *Ideas on Liberty,* October 2002, www.fee.org/vnews.php?nid=5188.

[3] Milton Friedman and Rose D. Friedman, *The Tyranny of the Status Quo* (Harcourt: New York, 1984).

[4] See, for example, Elliot Borin, "Private Info Becoming Plane Truth," *Wired News,* September 16, 2002, www.wired.com/news/politics/0,1283,55037,00.html. See also Robert O'Harrow Jr., "Intricate Screening of Fliers in Works; Database Raises Privacy Concerns," *Washington Post*, February 1, 2002. Some proponents of data-mining software regard it as equivalent to mind-reading. "'This is not fantasy stuff,' said Joseph Del Balzo, a former acting administrator of the Federal Aviation Administration and a security consultant working on one of the profiling projects. 'This technology, based on transaction analysis, behavior analysis, gives us a pretty good idea of what's going on in a person's mind.'"

[5] Quoted in John Markoff, "Pentagon Plans a Computer System that Would Peek at Personal Data of Americans," *New York Times,* November 9, 2002, www.nytimes.com/2002/11/09/politics/09COMP.html?tntemail0.

[6] See E.G. Ross, "Snoop Project," *The Objective American,* December 4, 2002, www.objectiveamerican.com/getbest.cfm?id=1263.

[7] Quoted in Markoff.

[8] Program Objective of the Total Information Awareness (TIA) System, www.darpa.mil/iao/TIASystems.htm. TIA is a project of the Defense Advanced Research Projects Agency (DARPA).

[9] See the TIA diagram archived by the Electronic Privacy Information Center at www.epic.org/events/tia_briefing/tia_categories.gif. Although the diagram was taken from the TIA web site, it appears to no longer be posted at that site. The creepy-looking "eye-in-the-pyramid" logo that aroused such furor and sardonic amusement among privacy advocates has also been removed. Its appropriate symbolism has been replaced by a more generic red triangle, sans the all-seeing eye.

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

[11] Ibid., p. 10.

[12] Ibid., p. 25.

[13] Ibid., p. 31.

[14] Bruce Mohl, "Large-scale identity theft is painful reminder of risk," *Boston Globe*, May 12, 2002.

[15] Garfinkel, p. 275.

[16] Jacob H. Fries, "Worker Accused of Selling Colleagues' ID's Online," *New York Times*, March 2, 2002.

[17] Garfinkel, p. 28.