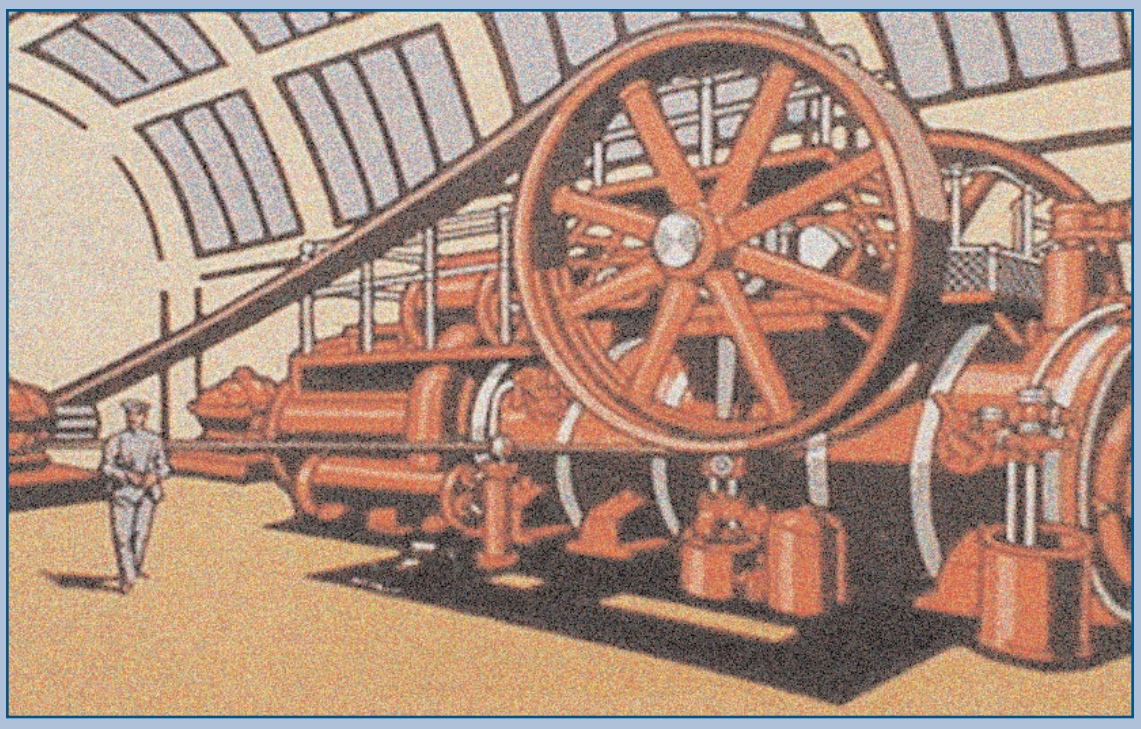
The Surveillance-Industrial Complex:

How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society



ACLU
AMERICAN CIVIL LIBERTIES UNION

August 2004

The Surveillance-Industrial Complex:

How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society

Published August 2004

Written by Jay Stanley

National Headquarters
125 Broad Street, 18th Fl.
New York, NY 10004-2400
(212) 549-2500

www.aclu.org

Table of Contents

Foreword

Not so long ago, our lives were mostly recorded on paper. From the doctor's office to the supermarket, any record of where we had gone or what we had done could only be tracked by looking at paper and ink. Today, however, the most intimate details of our personal habits and behaviors are now computerized. On millions of hard drives and microchips, more and more of what we do every day is recorded – not only by the government, but also by corporations. And as this report shows, when it comes to preserving our privacy, that is increasingly a distinction without a difference.

This special ACLU report, the 12th in our series on civil liberties since 9/11, paints a sobering picture of just how little control we have over our information today. It shows how information-age technology, anemic privacy laws and soaring profits have all combined to endanger our privacy rights to a point never before seen in our history.

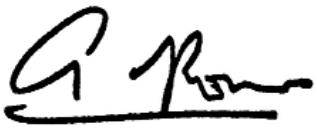
After you read this report, you will see that reform is clearly needed.

Americans from across the political spectrum understand that "the right to be left alone" is central to our constitutional democracy – that a secure sense of personal privacy is vital to preserving the openness of American life, and to protecting the boundless creativity, innovation and prosperity for which we are known around the world.

If we allow the fear of terrorism to create a new industrial base for surveillance technology, unfettered by reasonable and effective privacy constraints, these special characteristics of the American way of life will wither on the vine.

This report is packed with fascinating and frightening details about how the relationship between government and big business is changing before our eyes – or, all too often, behind our backs. Brought together, these details add up to a trend that would be almost hard to believe if it were not so well documented.

We at the ACLU are not sitting passively as the growth of a "surveillance-industrial complex" continues. I hope that you will read this report, and then join us to help stop it.



ANTHONY D. ROMERO
Executive Director
American Civil Liberties Union

THE SURVEILLANCE-INDUSTRIAL COMPLEX:

How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society

Introduction

Acting under the broad mandate of the "war" on terrorism, the U.S. security establishment is making a systematic effort to extend its surveillance capacity by pressing the private sector into service to report on the activities of Americans. These efforts, which are often costly to private businesses, run the gamut from old-fashioned efforts to recruit individuals as eyes and ears for the authorities, to the construction of vast computerized networks that automatically feed the government a steady stream of information about our activities.

Public-private surveillance is not new. During the Cold War, for example, the major telegraph companies – Western Union, RCA and ITT – agreed to provide the federal government with copies of all cables sent to or from the United States every day – even though they knew it was illegal. The program, codenamed "Operation Shamrock," continued for decades, coming to an end only with the intelligence scandals of the 1970s.

But even such flagrant abuses as Operation Shamrock pale in comparison to the emergence of an information-age "surveillance-industrial complex." The ongoing revolution in communications, computers, databases, cameras and sensors means that the *technological* obstacles to the creation of a truly nightmarish "surveillance society" have now been overcome. And even as this dangerous new potential emerges, our legal and constitutional protections against such intrusion have been eroded to a frightening degree in recent years through various court rulings as well as laws like the Patriot Act.

The ACLU has documented the confluence of these two trends in a separate report.[1] But there is a third crucial obstacle that the American security establishment is seeking to overcome in its drive to access ever more information about ever more people. That obstacle is the practical limits on the resources, personnel and organization needed to extend the government's surveillance power to cover hundreds of millions of people. There will always be limits to the number of personnel that the U.S. security state can directly hire, and to the "ratio of watchers to watched." This is the obstacle that the U.S. security establishment seeks to overcome by enlisting individuals and corporations as auxiliary members of its surveillance networks.

The advantages of privatized surveillance

Besides allowing the government to overcome the practical limits on its resources (what political scientists call "state administrative capacity"), the technique of folding private individuals and organizations into a government's surveillance network has several advantages for the government:

- It gives the government access to private-sector databases. Most of the interactions and transactions in Americans' lives are not conducted with the government, but with corporations and other private entities, who therefore hold most of the details of Americans' lives – including much of what is private and important to them.

- It lets the government create a system of "distributed surveillance" or "swarm intelligence" in which scattered, individual, independent sources of information are brought together to create a big picture that the government could never construct directly.

- It shifts costs from government to the private sector by forcing companies to take expensive steps such as hiring additional staff to meet information collection and analysis mandates – in effect, imposing a hidden "surveillance tax" on those companies.

- It creates constant uncertainty whenever people are in a situation where an informant might be present, enormously amplifying the effect of government surveillance on individual behavior and psychology.

- It offers what is often a path of least resistance to working around privacy laws. Our laws have historically protected information held by an individual, while information held by third parties was either assumed to be innocuous or protected by professional codes of confidentiality. But today, third-party information has become far more comprehensive and significant.

- It allows the government to carry out privacy-invading practices at "arm's length" by piggy-backing on or actually cultivating data collection in the private sector that it could not carry out itself without serious legal or political repercussions.

The privatization of government functions has always been a popular way of doing business in the United States, and surveillance is no exception.

In this report, we look at many aspects of this trend – drawing together and setting in context many stories that in isolation might seem far less significant. The elements we examine are:

- Recruitment and exhortation of individuals to serve as eyes and ears for the authorities.

- Government recruitment of corporations and other private-sector organizations by forcing them either to turn over their customer databases, gather and store information in ways useful to the government or join regularized systems for reporting on individuals.

- Growing government partnerships with private-sector companies that specialize in building dossiers about individuals.

- Lobbying by companies in favor of increased surveillance.

The privatization of government functions has always been a popular way of doing business in

the United States, and surveillance has been no exception. There is a long history of cooperation between government security agencies and private-sector surveillance programs, from private "detective" agencies like the Pinkertons, which helped employers battle the labor movement in the 19th century, to the "corporate officials, labor spies, super-patriots, amateur detectives and assorted vigilantes" who worked with the government to combat radicalism after World War I and remained active in various forms right through the last years of the Cold War.[2]

But nothing in our past compares to the efforts at distributed mass-surveillance that are now underway, which combine the long-standing police impulse to expand private-sector information sources with awesome new technological capabilities for vacuuming up, storing and keeping track of vast oceans of information.

Recruiting Individuals

Homeland security starts at home.
– U.S. Citizen Corps

In January 2002 the Justice Department announced the creation of a program called the "Terrorism Information and Prevention System," or TIPS. Billed as "A national system for concerned workers to report suspicious activity," the program would have recruited "millions of American truckers, letter carriers, train conductors, ship captains, utility employees and others" as government informants.[3] The proposed scope of this project was stunning – it would have recruited, in its pilot program alone, one million informants in just 10 cities – or one in every 24 Americans living in those cities.[4] Many of those targeted for inclusion in the scheme were workers with access to Americans' homes – utility workers, letter carriers and cable technicians – who were to report to the government anything that they considered an "unusual or suspicious activity."

The recruitment of informants for particular investigations has long been a key tool of law enforcement, but only under the most oppressive governments have informants ever become a widespread, central feature of life. The East German Stasi, for example, not only employed 91,000 full-time workers, but also recruited from among the citizenry more than 170,000 non-professional informants, or as many as one in every 50 citizens, to spy and report on their fellow citizens. Stasi agents even used blackmail and other pressure tactics to get people to spy on their own family members. The result was to create a pervasive sense of mistrust that prevented citizens from sharing their complaints with each other, gaining strength from connecting with others of like mind and challenging those who were in power.

A massive effort is underway to turn regular Americans into untrained government monitors.

Few believe that the U.S. will ever become a state like East Germany. But the TIPS proposal was rightly met by a storm of outrage, and the government quickly moved to eliminate the inclusion of workers who visit Americans' homes. Even in its reduced form, however, Congress shut it down.

But while TIPS proved short-lived, it was only the most blatantly offensive and direct example of an idea – organizing private individuals to increase the government's surveillance capacity – that continues to live on. A massive effort is underway to turn regular Americans into

untrained government monitors who, pressed by constant urgings for vigilance and suspicion and lacking the training or accountability of professional law enforcement officers, are asked to report to the authorities anything they think is "unusual or suspicious."

Some directives emanating from the government are undoubtedly beneficial, such as instructions on how to prepare for civil emergencies, and certainly there is nothing wrong with the authorities making rational requests for citizens' help. But the new warnings are enormously vague and broad, yet frightening and intense. Unlike "wanted" posters and other traditional public appeals, they are based not on crimes that have already been committed, but on the prospect or suspicion that an individual might be planning something bad. Many "suspicious behaviors" cited by the authorities have no rational or proven relationship to terrorism – and in fact, it is doubtful that there are such things as clearly defined behavioral predictors of terrorism.

Many "suspicious behaviors" cited by the authorities have no rational or proven relationship to terrorism.

These kinds of broad directives leave a much wider scope for racial profiling and paranoia directed at anyone who is different or stands out – and are likely to generate large numbers of false positives that will swamp any useful information that might be obtained. In addition, none of these programs can be viewed apart from the larger context: a world where government has interrogated, fingerprinted and detained thousands of people based on their ethnicity.

The government's constant exhortations to micro-vigilance, if taken to heart, will create an atmosphere of conformism and mistrust that encourages abuses, divides Americans from one another and casts a chill over the traditionally freewheeling nature of American life.

"Watch" programs

When President Bush called for the creation of TIPS in his 2002 State of the Union address, it was just one element of a larger program called the "Citizen Corps" that is aimed at giving Americans a chance to get directly involved in homeland defense. Bush also called for "Neighborhood Watch" programs to be doubled in number and expanded beyond their traditional role of deterring and detecting household burglary to "make them more attuned to preventing terrorism."[5] The means for carrying this out is a push to encourage the formation of "Citizen Corps Councils" around the nation. Citizen Corps materials urge Neighborhood Watch participants to "train family members on identifying suspicious behaviors that could indicate terrorist activity."[6]

The Citizen Corps home page still proclaims that its mission is to "harness the power of every individual through education, training and volunteer service to make communities safer, stronger and better prepared" for terrorism and other threats.[7] And indeed, though Congress may have ordered TIPS shut down, the government continues to run several programs that are very close in nature to TIPS.

"Be our eyes and ears so we can calm your fears."

– River Watch slogan

- **Marine Watch programs.** A Maine program dubbed "Coastal Beacon," recruits fishermen and members of the general public to keep a watch out for "suspicious activity."[8] The fact

that this program does exactly what Congress banned under TIPS was confirmed by President Bush himself, who declared Coastal Beacon "one of the most innovative TIP [*sic*] programs in the country."[9] An Ohio program called "Eyes on the Water" urges boaters to report "unusual behavior when you see it." As one Coast Guard officer told a reporter, "A guy who is not wearing the right gear or fishing in an unusual location – let us know about it." A program in Michigan called "River Watch" has as its slogan, "Be our eyes and ears so we can calm your fears."[10]

- **Highway Watch.** Another TIPS program that has outlived TIPS is "Highway Watch," under which truck drivers are taught to recognize "highway dangers" and report them to a central dispatch center. The program has a heavy homeland security element – indeed, it is being funded by the Department of Homeland Security (DHS). A program fact sheet boasts that the more than three million truck drivers on the roads make up "a potential army of eyes and ears to monitor for security threats." Not only are drivers "naturally very aware of suspicious activity and behavior," but "truck drivers are everywhere – ports, airports, malls, bridges, tunnels – thus giving greater range to homeland security observation efforts."[11]

- **"CAT Eyes."** A program called "Community Anti-Terrorism Training Institute," or "CAT Eyes," is working to "educate citizens in the civilian community to be effective eyes and ears for potential terrorist activities." Embraced by police departments from across the eastern U.S., it aims for the formation of hierarchically structured "neighborhood block watches" including "Neighborhood Coordinators," "Block Captains" and "Block Watchers," each of whom "acts as eyes and ears for law enforcement and reports any suspicious activity." The program's motto is "watching America with pride not prejudice."[12]

- **Real Estate Watch.** Police outside Cincinnati have set up a pilot program in which the police train real estate agents "how to be observant." The realtors keep their eyes open for suspicious activity as they make their rounds, based in part on alerts provided by the police, and report back anything suspicious they see.[13]

- **Florida's TIPS.** In a direct local imitation of the original TIPS concept, police in Orange County, Florida are planning to train emergency personnel, cable workers and other public and private workers to look for and report evidence of terrorism, drug trafficking, or child pornography in private homes. Overseen by Florida state police officials, the program's brochure originally included an element of explicit racial profiling. Though that was removed, the program is still underway, leaving homeowners to wonder if anything in their home might draw suspicion whenever a cable or utility worker comes in to do a repair.[14]

- **Other State Reporting Programs.** Many states and localities appear to have citizen reporting programs in place. New York, for example, has instituted a "Statewide Public Security Tips Hotline" the public can use to report "suspicious or unusual behavior" to the police. "In protecting our homeland security," declared a September 2002 news release on the program, "the public should consider themselves partners with our local, state and federal law enforcement agencies." All tips, however raw, "will be cross-referenced through federal, state and local databases." There is no mention of whether the name of an innocent person who is the subject of a tip will ever be purged from the record.[15]

Privacy safeguards are rarely created by security agencies on their own without intense outside pressure.

In fact, it is far from clear what any of these programs do with information about "suspicious" individuals that they receive – how reports are recorded, shared and stored in domestic intelligence or law enforcement databases or what is done to ensure that innocent individuals who are the subjects of raw suspicions and rumors will not have a permanent black mark associated with their names in some government database. Experience has shown that such safeguards are rarely created by security agencies on their own without intense outside pressure.

A disturbing sub-genre of TIPS-like programs are those run by the military. They include:

- **"Eagle Eyes."** This program is billed as "an anti-terrorism initiative that enlists the eyes and ears of Air Force members and citizens in the war on terror." In addition to a telephone tip line, the program offers training in how to detect terrorist activity. "Anyone can recognize elements of potential terror planning when they see it," boasts the program's Web page. Things to watch for include "People who don't seem to belong in the workplace, neighborhood, business establishment or anywhere else. . . . If a person just doesn't seem like he or she belongs, there's probably a reason for that."[16]

- **"Talon."** According to an internal memo obtained by *Wired News*, this Pentagon database contains "raw, non-validated" reports of "anomalous activities" within the United States, and provides a mechanism to collect and share reports "by concerned citizens and military members regarding suspicious incidents."[17]

The Pentagon says the purpose of the Talon system is to protect Defense Department property and personnel. Of course, since a terrorist could try to attack those targets just like any others in the U.S., there is no limit to the amount of domestic surveillance that could be justified by that rationale. Interestingly, the same rationale of "base protection" was given when it was discovered that the Army was involved in the construction of dossiers about millions of U.S. airline passengers (see p. 10). All this in a context where, as one expert puts it, the military is acting to "break down long-established barriers to military action and surveillance within the U.S."[18]

A disturbing sub-genre of TIPS-like programs are those run by the military.

Citizen vigilance

Beyond these organized watch programs are more diffuse campaigns of "citizen awareness" featured on government Web sites around the nation. These campaigns

urge Americans to be suspicious, and to report to the authorities anyone who fits a long list of suspicious characteristics. State and local governments have posted or linked to reams of materials that one way or another warn and instruct citizens "how to be vigilant."[19]

Examples of this kind of material abound:

- A flyer from the Maryland State Police asks citizens to be alert for "anyone who does not appear to belong."[20]

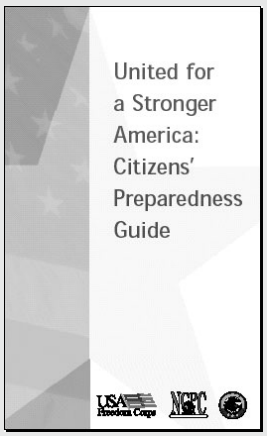
- The residents of Lucas County, Ohio, and many other localities around the country are admonished in materials prepared by the DHS to look for "persons not fitting into the surrounding environment," including any "beggar, demonstrator, shoe shiner, fruit or food vendor, street sweeper, or a newspaper or flower vendor not previously recognized in the area," who, it is explained, could be a terrorist in disguise.[21]

Predictably, the tip centers that have been set up are already attracting malicious tips.

- Messages on electronic highway signs in Virginia and Maryland list toll-free phone numbers and ask drivers to "Report Info on Terrorism" and "Report Suspicious Activity" – solicitations that leave many citizens puzzled over just how they are supposed to act on them.[22]

- A widely distributed version of DHS's color-coded terrorism "Homeland Security Advisory System" tells citizens to be "watchful for suspicious activities."[23]

The Citizens' Preparedness Guide



A significant example of citizen "lookout literature" is a "Citizens' Preparedness Guide" published by the federal Citizen Corps. After an introduction in which Attorney General John Ashcroft declares that "your country has never needed you more," the guide urges Americans to "be alert as you go about your daily business" and "learn the normal routines" in order to "help you to spot anything out of place." Citizens should be "on the lookout" for suspicious activities "in your neighborhood, in your workplace, or while traveling" – in short, everywhere. When it comes to the Internet, famous for being home to every imaginable activity, viewpoint, hobby and fetish, Americans are told to "report unusual activities to the authorities."

In addition to directing Americans to "keep your yard clean" and "prune shrubbery," the guide asks citizens to contact the FBI "immediately" if they "observe a pattern of suspicious activity," including "someone unfamiliar to you loitering in a parking lot."

Concludes the guide, "Homeland security starts at home."[24]

- A Coast Guard Web site lists "suspicious activity" that includes the distribution of "Anti-American pamphlets, or flyers"[25] – certainly an invitation to abuse, considering how broadly the label "Anti-American" has been applied in the past. (In addition, it is unlikely that a genuine terrorist planning an attack would call attention to himself by leafleting beforehand.)

Implicit racial profiling

Predictably, the tip centers that have been set up are already attracting malicious tips from individuals "turning in" neighbors they dislike, tips about strangers engaging in "un-American activity" and of course many reports based on racial profiling. "We've gotten calls from people who've seen someone who looks Middle Eastern in the store or library, maybe on the computer," a Virginia police official told the *Chicago Tribune*.[26]

The government is increasingly circumventing those restrictions simply by turning to private companies.

In fact, the generality of many of these warnings and reminders may be explained by an implicit element of racial profiling. Does the Coast Guard really want to receive reports on every "guy who is not wearing the right gear or fishing in an unusual location"? Or just when that "guy" happens to be of Middle Eastern appearance?

Truckers anxiously watching the highways, boat owners watching the shores, individuals constantly urged to watch for people who don't fit in – together it adds up to a vision very close to what was envisioned under the supposedly discontinued TIPS program.

Recruiting Companies

We regret to inform you that we have decided that it is not in our best interest to continue your banking relationship with us.
– Letter from Fleet Bank to U.S. citizen Hossam Algabri

As disturbing as the government-sponsored informer programs are, even more alarming is the government's recruitment of companies and other independent organizations into its growing surveillance machinery. The Privacy Act of 1974, although riddled with exceptions and loopholes, does restrict the ability of law enforcement agencies to maintain dossiers on individuals who are not suspected of involvement in wrongdoing.[27] But the government is increasingly circumventing those restrictions simply by turning to private companies, which are not subject to the law, and buying or compelling the transfer of private data that it could not collect itself.

A long history of private-sector surveillance

The U.S. government actually has a long history of turning to the private sector for help in gathering information on individuals. Examples include:

- **The Western Goals Foundation.** In Los Angeles, thousands of files on activists of all kinds were ordered destroyed in the wake of the revelations of domestic spying in the 1970s. But in 1983 these raw intelligence files were discovered hidden away in the garage of an LAPD detective, who had been sharing them with the Western Goals Foundation, a Cold War anti-communist group that used the files to build private dossiers on progressive political activists around the nation. Western Goals acted as a

private "clearinghouse" of dossiers on political activists from police agencies in different states – collecting, disseminating and "laundering" the sources of that information.[28] The group circulated information – much of it false and defamatory – about those activists not only to local police departments, but also to numerous federal police agencies including the Secret Service, the FBI, the State Department and the CIA.[29]

- **The "San Diego Research Library."** In another case, a retired military intelligence officer named Ralph H. van Deman established a legendary data collection facility in California, which kept dossiers on religious, labor, civil rights and other activists. For over 30 years beginning in 1929, this "private" facility, operated with the support of private donors, the state of California and the Army, maintained 200,000 files based in part on confidential information provided by volunteer informers. The facility regularly exchanged material with federal and state intelligence agencies, and thus served as a quasi-governmental intelligence agency.[30]

- **Operation Shamrock.** Perhaps the ultimate example was the Cold War program called "Operation Shamrock," in which the major U.S. telegraph companies "secretly turned over to the NSA, every day, copies of all messages sent to or from the United States."[31] As described by reporter and author James Bamford, the program began in 1945 when the presidents of the telegraph companies all agreed to participate after the government appealed to their patriotism. They took part knowing that their actions were illegal and against the uniform recommendations of their own corporate attorneys.[32] When the carriers computerized their operations in the 1960s, Operation Shamrock gained the ability to conduct keyword searches through each day's traffic. At that point, the NSA increasingly began to scan the nation's telegraphs against long lists of surveillance targets provided to the NSA by other security agencies – including American anti-war and civil rights protesters, and even such groups as the Quakers.[33]

The potential is greater today

But even abuses like Operation Shamrock pale in comparison to what is possible with today's technology:

- **Computer hardware and software is far more sophisticated.** Unwieldy tape reels have been replaced by swift and massive hard drives, and software today can, with increasing reliability, transcribe spoken words or analyze meaning based on the context of a communication.

- **More business is conducted electronically.** Because of the convenience of cell phones, the Internet and other innovations, the amount of business that Americans conduct via electronic communication has vastly increased.

The threat posed by government collection of third-party information is far greater today than it would have been in the 1950s, or even the early 1990s.

- **Corporations are gathering more data for their own reasons.** Companies have discovered that information about customers has enormous cash value – and now have on hand cheap new technologies for collecting, storing and sharing such data. Americans are increasingly finding themselves pestered for personal

details at every turn, or routinely tracked through stratagems like supermarket loyalty cards – all for the purpose of building a financially valuable record of their lifestyle and habits.[34]

To obtain information about individuals' activities, the government often need do no more than ask.

The result of these developments is that the threat posed by the systematic government collection of personal information held by corporations and other third parties is far greater today than it would have been in the 1950s, or even the early 1990s.

Many options for accessing private data

The bottom line is that the private sector is tracking more and more of our activities for its own purposes, and the government is free to leverage this private collection as a way of extending its own powers of surveillance. The government has an array of options for accessing third-party information. It can:

- Ask for data to be shared voluntarily.
- Simply buy information.
- Demand it, using legal powers granted by the Patriot Act and other laws.
- Use laws and regulations to dictate how private-sector data is handled and stored in order to increase its surveillance value for the government.
- Create regularized systems for standing access to records of private activities.

Corporate compliance with government data-surveillance efforts ranges from unwilling resistance to indifferent cooperation to eager participation to actual lobbying of the government to increase such activities. But with a range of options at its disposal, the government can acquire a rich stream of information about private activities from any source. These techniques add up to a startling advance in government monitoring of American life. Let us examine each of them.

Companies may be afraid to turn down "voluntary" requests because they fear regulatory or law enforcement scrutiny of their own activities.

Voluntary sharing of data

To obtain information about individuals' activities, the government often need do no more than ask. Many companies are willing to hand over the details of their customers' purchases or activities based on a simple request from the FBI or other authorities. Some companies believe they are being patriotic; others may be afraid to turn down "voluntary" requests because they fear regulatory or law enforcement scrutiny of their own activities; others may simply be eager to please.

Multiple airlines have admitted turning over the records of their customers' travels to the government. In each case, the information was turned over not to help the government solve a particular crime or track a particular suspect, but in order to examine each traveler's records in the hopes of identifying terrorists by detecting "suspicious" patterns in his or her travels – in effect, turning every traveler into a suspect (see discussion of data mining, p. 23).

- At the request of an official now at DHS, the airline JetBlue gave a Pentagon subcontractor more than 5 million passenger records, which were combined with detailed personal files on each passenger purchased from a "data aggregator" company called Acxiom.[35]

- When the JetBlue story broke, Northwest Airlines said it had not shared its passengers' records, but a few months later it was discovered that in fact, it had given millions of passenger records to NASA.[36]

- In April 2004, American Airlines admitted that it, too, had shared passenger records (1.2 million of them) with the TSA and four research companies.[37]

- In May 2004 the nation's largest airlines, including American, United and Northwest, also admitted giving millions of passenger records – up to a year's worth – to the FBI after the 9/11 attacks.[38]

Other known recent examples of "voluntary" data sharing with the government include:

- **Scuba shops.** In May 2002 the Professional Association of Diving Instructors voluntarily provided the FBI with a disk containing the names, addresses and other personal information of about 2 million people, nearly every U.S. citizen who had learned to scuba dive in the previous three years.[39]

- **Colleges and universities.** A 2001 survey found that 195 colleges and universities had turned over private information on students to the FBI, often in apparent violation of privacy laws; 172 of them did not even wait for a subpoena.[40]

- **Travel companies.** A 2001 survey of travel and transportation companies found that 64 percent had provided customer or employee data to the government, many of them in violation of their own privacy policies.[41]

These are only some of the examples that have come to light; as the airline examples indicate, companies that have shared information are often far from open about it.

There is a long and unfortunate history of cooperation between government security agencies and powerful corporations to deprive individuals of their privacy and other civil liberties.

InfraGard – a corporate TIPS program?

A more systematic example of voluntary cooperation is a partnership between the FBI and private corporations called "InfraGard." This program is aimed at encouraging "the exchange of information by the government and the private sector members" to protect against terrorism and other threats to the nation's infrastructure.

The program has more than 10,000 members organized into 79 local chapters; the list of participating companies is kept secret. Members wishing to participate fully must undergo a security check and obtain clearance by the FBI.[42] The *Cleveland Plain Dealer* described it as a "a vast informal network of powerful friends," a "giant group of tipsters" created by the FBI under a "philosophy of quietly working with corporate America" in order to "funnel security alerts away from the public eye and receive tips on possible illegal activity."[43]

It is not clear what kind of information sharing takes place under InfraGard. The program was created as a means of stopping cybercrime, but has broadened to cover threats of all kinds to the nation's "critical

infrastructure." The program's Web site suggests that it simply gives the FBI a quick way to spread specific, credible security alerts to companies that may be targets, and gives companies a discreet way to report attacks by hackers.

But there is evidence that InfraGard may be closer to a corporate TIPS program, turning private-sector corporations – some of which may be in a position to observe the activities of millions of individual customers – into surrogate eyes and ears for the FBI. For example, several program members told the *Plain Dealer* that "they received through InfraGard a list of Web sites frequented by terrorists and were monitoring their computer networks to see if anyone on their systems visited those pages."[44] It is also possible that the program serves as a more controlled version of the FBI's watch list distribution program "Project Lookout" (see p. 19).

The government has a powerful arsenal of legal weapons with which to force third parties to provide access to individuals' records.

There is a long and unfortunate history of cooperation between government security agencies and powerful corporations to deprive individuals of their privacy and other civil liberties, and any program that institutionalizes close, secretive ties between such organizations raises serious questions about the scope of its activities, now and in the future.

Purchasing data on the open market

Another option open to government agencies seeking information on individuals is to simply purchase it on the open market. As private-sector information-gathering has exploded in recent years, so has the amount of data that is now available to the government (and any other customer) willing to pay the price. Although government information-purchasing was once a minor matter, the explosion of private-sector data collection has begun to significantly undermine the laws meant to protect Americans from government snooping.

Perhaps the ultimate example of the powerful information sources now available for purchase by the government is the existence of companies called data aggregators, which make it their business to gather, compile and distribute dossiers full of information about Americans' personal lives (see p. 25).

Plentiful legal powers to demand private-sector data

If a company won't donate or sell its data on individuals, the government has a powerful arsenal of legal weapons with which to force it (as well as other entities such as doctors' offices and libraries) to provide access to individuals' records in its possession.[45] Even as private-sector companies hoard more and more details about our transactions, the government's powers to obtain that data are growing:

- **The Patriot Act.** The Patriot Act makes it much easier for the government to demand information from businesses and lowers the standard of evidence required for such demands. Section 215 of the act, for example, gives the FBI the power to demand customer records from Internet service providers (ISPs) and other communications providers, libraries, bookstores or any other business – with little judicial oversight. The businesses can be banned from telling anyone, including their affect-

ed customers, about the search. And the search orders do not even have to specify a particular target.[46]

- **National Security Letters.** These obscure devices, which can be written by FBI officials in field offices without the approval of a judge, give the government broad power to demand records. Once upon a time this sweeping power could only be used to get information about "agents of a foreign power" from banks, credit agencies and Internet service providers. But the Patriot Act changed the law to allow their use against anyone, including persons not suspected of a crime.[47] And a bill quietly signed into law by President Bush in December 2003 extends coverage to a wide variety of businesses, ranging from jewelry stores to stockbrokers to car dealerships to casinos.[48] Businesses are also subject to a gag order prohibiting them from talking about the government's data demands.

Law enforcement is increasingly forward-looking - trying not just to solve crimes but to anticipate and prevent them.

Most restrictions on the use of information in government databases have exceptions for law enforcement and intelligence purposes. The scope of those exceptions was once clear: It was limited to attempts to solve crimes, and to stop foreign espionage. But under the new, post-9/11 security paradigm, which more than ever before views every American as a potential suspect, those exceptions may now be far wider than was ever intended when they were written into the law. Law enforcement is increasingly forward-looking – trying not just to solve crimes but to anticipate and prevent them. And the boundaries between foreign intelligence and domestic law enforcement have come under sustained assault.[49]

Already "fishing" with new powers

The government's expanded surveillance powers are, in fact, being used. Phone companies, banks and retail stores report more requests by law enforcement for information about customers:[50]

- In December 2003, the FBI presented national security letters to hotels in Las Vegas and obtained access to names and personal information on all their customers between December 22 and New Year's Day. The FBI also vacuumed up information on anyone who flew into the city, rented a car or truck or patronized a storage facility. The FBI thus indiscriminately scrutinized the lawful activities of an estimated 270,000 Americans based on no individualized suspicion of wrongdoing.[51] (Ironically, the incident came as the city was conducting an advertising campaign based on the slogan, "what happens here, stays here.")

- Since passage of the Patriot Act, the FBI has been using national security letters very aggressively in general, according to a January 2003 list obtained through a Freedom of Information Act request filed by the ACLU. The list was blacked out – but it was six pages long.[52]

- Internet service providers report that search orders have "gone through the roof."[53] ISPs maintain records of individuals' Internet use, including records of IP addresses (a number that is assigned to each computer that connects to the Internet) that can be combined with logs automatically maintained by most Web servers to identify which individuals have

visited a Web site, participated in "anonymous" chat or message boards or adopted a particular online pseudonym. In 2002 alone, for example, BellSouth received about 16,000 subpoenas from law enforcement and 636 court orders for customer information.[54]

- Attorneys who represent many of the affected companies report that it is not just the number of requests that is increasing, but also their scope; more requests take a "shotgun approach" or are "just fishing."[55]

What happens to all of this data when the authorities complete the investigation for which it was collected? As one former high-ranking intelligence official observed, "The FBI doesn't throw anything away."[56]

In addition, private companies often do not have the time, resources or inclination to "minimize" the data that they hand over to the government. Instead of turning over just the names of its customers, for example, a hotel might find it easier to simply hand over its complete files, including all the details of customers' transactions.

Building in surveillance

In addition to requesting, purchasing or ordering the supply of private-sector data, the government is also taking steps to ensure that nothing is left to chance when it needs information from a particular company or industry. By affirmatively guiding, structuring or mandating the maintenance of information on individuals by private organizations, the government is ensuring that its agents will get what they want when they go looking for it.

The government is taking steps to ensure that nothing is left to chance when it needs information from a particular company or industry.

CALEA

An early example of this trend is the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which forced telecommunications providers to design their equipment according to the FBI's specifications in order to make eavesdropping easier and more convenient – in effect, requiring the architects of the nation's newest communications networks to twist those networks into designs that they would not otherwise take, simply to preserve the government's ability to eavesdrop. It is the constitutional equivalent of the government requiring that all new homes be built with a peephole for law enforcement to look through.

Recently, the FBI and other law enforcement agencies have sought to expand CALEA even further. They have pushed for an aggressive interpretation of the statute that would allow it to monitor certain Internet content without a warrant, and to collect tracking information about the physical locations of cell phone users – turning cell phones into what, for all practical purposes, are location tracking bugs (a use that many, including the ACLU, assert is not authorized at all by CALEA).

And now, the FBI is also trying to force broadband Internet providers to build their technical systems in a way that will allow the government to eavesdrop on Internet telephone calls.[57] The fledgling Internet phone industry is still experimenting with a variety of technologies, yet the government would force companies to give law enforcement a ground-floor veto over the specifications of new products they develop – before they've even worked out the bugs or tested their success in the marketplace.

Mandatory data retention

Around the time that the FBI pushed for and won the surveillance-enabling CALEA statute, it also made a push for a national "data retention" law, which would have forced ISPs and other communications providers to retain their records of individuals' communications for a set period of time just in case those records should prove helpful in an investigation. More recently, there were reports that an early draft of the Bush administration's "National Strategy to Secure Cyberspace" called for a mandatory customer data retention regime.[58]

In a legal environment where the government has very few limits on its ability to access information about individuals that is stored by third parties such as ISPs, a data retention law requiring such storage would short-circuit one of the few true privacy protections left – the disposal of records once they are no longer needed.

The U.S. has pushed the European Union to adopt data retention laws. In October 2001, for example, President Bush himself directly asked the EU to change its rules to allow for the retention of communications traffic data.[59] It is being adopted by 9 of the 15 EU member states.[60] This is a perfect example of what has been called "policy laundering" – the act of pushing laws through foreign and international bodies that could never win direct approval at home.

Americans have long feared the specter of the government maintaining dossiers filled with information about the lives of individual, innocent citizens. Data retention, whether mandatory or de facto, achieves the same goal indirectly, by ensuring that information is stored by corporations – from where, as we have seen, it can easily be accessed by the authorities.

Airline Profiling

Another example of this dynamic can be found in airline profiling proposals such as the CAPPS II program, under which the government would conduct background checks on every traveler in order to give him or her a "risk assessment" rating of "red," "yellow" or "green." CAPPS II would require the airlines to collect and furnish to the government each passenger's full name, address, phone number and date of birth when they make a reservation. Computer systems in use today are not built to track – they are unable to tell if the John Doe who took one flight is the same Jonathan Doe who took another, and the same J.S. Doe Jr. who took a third. By imposing a standardized data-collection requirement, the government will make it easy to compile lifetime travel dossiers covering everyone who flies anywhere in the world.[61]

The U.S. has pushed the European Union to adopt data retention laws.

The Computer Reservation Systems – independent contractors that handle reservations for almost all airlines – are under absolutely no legal obligation to protect the privacy of that information. They do not have direct relationships with actual travelers, and thus have no consumer privacy policy by which they must abide (or market pressure for good privacy practices). And no U.S. privacy laws restrict their ability to compile, store and share their dossiers on individuals' travel.

And of course, there are plenty of laws that would give the DHS and other government agencies easy access to these travel dossiers – if the CRSs don't simply sell them access outright.[62]

In July 2004, Homeland Security Secretary Tom Ridge seemed to indicate that the CAPPS II program would be terminated. Other DHS officials, howev-

er, indicated that while the CAPPS name may be retired, the concept will live on. As one spokesperson put it, "The process of creating an automated passenger pre-screening system. . . will continue."[63]

Whether through CAPPS II or some other passenger-profiling system, it is clear that the government once again wants to make sure that personal data will be waiting in private hands (and in a suitable form) when agents want it.

Through the Patriot Act, the government has created a system for the near-total surveillance of the nation's financial system.

The Patriot Act: Drafting industry into the government's surveillance net

As we have seen, the government has many options for accessing particular pools of information. Other developments, however, are potentially even more frightening than the government's free hand in gathering data on particular targets. Increasingly, the government is working to construct systematic mechanisms that provide constant feeds of (or open access to) private-sector data. Such systems truly turn private companies – in some cases, entire industries – into agents of the surveillance state.

The new focus on "terrorist financing activities" potentially involves much deeper scrutiny of everyday financial transactions than has been previously conducted.

A prime example of such a system is the growing machinery for government monitoring of financial activities, which has been enabled by the Patriot Act and justified by the need to stop money laundering. Through the Patriot Act, the government has created a system for the near-total surveillance of the nation's financial system:

- It expanded a system for reporting "suspicious" financial transactions.
- It set up a system for the government to conduct broad-ranging, nationwide "Google searches" through financial records.
- It required financial institutions to set up an identity verification process.
- It required financial institutions to check their customers against government "watch lists."

These steps involve the increased use of tools that were originally created to catch drug dealers and other traditional criminals in the fight against terrorism. But as a Federal Reserve official pointed out to Congress,

> Terrorist financing activities are unlike traditional money laundering in a very significant respect. Money used to finance terrorism does not always originate from criminal sources. Rather, it may be money derived from legitimate sources that is then used to support crimes. Developing programs that will help identify such funds before they can be used for their horrific purposes is a daunting task.[64]

In short, the new focus on "terrorist financing activities" potentially involves much deeper scrutiny of everyday financial transactions than has been previously conducted, because it involves searches of "money derived from legitimate sources" and scrutiny of individuals who have not committed any crime.

Expanded system for reporting "suspicious" financial transactions

The nation's financial companies have been enlisted into an enormous effort to provide a steady stream of routine financial information to the government. Under the Bank Secrecy Act of 1970, every bank, thrift and credit union is required to file a report with the government whenever a customer deposits $10,000 or more. The Patriot Act has dramatically expanded that requirement, stating that "any person who is engaged in a trade or business" – meaning every shop owner, plumber, consultant, home-improvement contractor and so on – who receives $10,000 or more in cash must file a detailed report, called a "Suspicious Activity Report," with the government.[65]

The nation's financial companies have been enlisted into an enormous effort to provide a steady stream of routine financial information to the government.

Among the problems with this system:

- While $10,000 may seem like a lot of money, it's not as much as it used to be, and the law contains no provision indexing this reporting threshold to inflation. If, when this law was originally passed in 1970, the threshold had been set at a level equivalent to $10,000 of today's spending power, it would be just $2,625 today. In effect, the threshold for reporting to the government has been lowered by nearly 75 percent. And if this law had been passed at the corresponding level in 1932, the threshold today would be just $855.[66]

- Those affected the most may be immigrants and minorities, who tend to use the traditional banking system the least (and therefore, when making a large purchase, are less likely to be able to write a check).

- Given the lack of privacy protections for credit card records, which are routinely shared by financial institutions, cash is the only recourse for those who want to preserve their privacy when making a purchase.

- It's far from clear how effective this system will be at its stated goal of stopping money laundering. "You're trying to turn an untrained populace into the monitors of money laundering activity," according to financial regulation expert James Rockett. "If you want to stop this, it's got to be done with police work, not tracking consumers' buying habits."[67]

With all this information pouring into an enormous government database of financial transactions, the effect will be continuous government monitoring of an ever-growing proportion of individuals' economic activities.

A system for government "Google searches" through Americans' private financial records

Even more powerful than the "Suspicious Activity" reporting requirement is a set of government regulations (stemming from Section 314 of the Patriot Act) that force financial institutions to check their records to see if they have engaged in any transactions with "any individual, entity or organizations listed in a request submitted by" the government. This grants any arm of govern-

Any arm of government with a law enforcement function can now order a search of financial institutions across the nation for records matching a suspect.

ment with a law enforcement function – including even agencies such as the Agriculture Department and the Postal Service – the power to order a search of financial institutions across the nation for records matching a suspect.

These searches can be done to investigate any suspected cases of money laundering – an extremely broad offense that encompasses any effort to disguise illicit profits, and can be used in pursuit of more than 200 different crimes. According to figures obtained by *Newsweek*, in 2003 alone the government used the Patriot Act to conduct searches on 962 suspects – and two thirds of the documents obtained were for money laundering cases that had no apparent connection to terrorism.[68]

Of course, the names of suspects that the government runs by financial institutions can presumably be retained by those financial institutions, and nothing prevents them from blacklisting those individuals and refusing to give them loans or otherwise do business with them, even if they are perfectly innocent of any wrongdoing.[69]

The unprecedented effect of these rules is to create and put at the government's fingertips an enormous distributed database of every transaction recorded by a financial institution in the United States.

New ID requirements

Completing the circle of the government's systematic enlistment of financial companies in its surveillance web is Section 326 of the Patriot Act, which requires that such companies create a "Customer Identification Program" of strict identity checks. The law requires that when any customer opens an account, takes out a loan, obtains a credit card or performs any other financial business, the financial institution must obtain and verify the customer's name, address, date of birth and social security number. Usually this is done by demanding a picture ID. Furthermore, the law imposes a data-retention requirement, mandating that companies keep records of identity verification for five years past the closure of an account.[70]

This provision protects and enhances the government's other powers to search through financial records by seeking to ensure that those records can be consistently linked to all the other records that exist about an individual. Of course, like all ID-checking requirements, this is ultimately a futile measure against any even minimally motivated bad actor.

The Patriot Act mandates that companies transform themselves into surrogate agents for the government.

Watch list checks

Once financial institutions have verified a customer's identity, they face another significant requirement imposed by Section 326 of the Patriot Act: They must check whether the person is on a government list of known or suspected terrorists or other watch lists. This requirement goes beyond simply acquiring information from the private sector; it actually mandates that companies transform themselves into surrogate agents for the government, required to constantly watch for anyone listed on one of the government's lists of suspected terrorists.

Individuals must now be checked against terrorist watch lists whenever they buy or sell property – including jewelers, pawnbrokers, and even average families buying or selling a home.[71]

Watch list searches can and do cause real harm to people. For example:

- An American citizen named Hossam Algabri received a statement in late 2002

from Fleet Bank discontinuing his account. The bank would not tell him what the problem was, except that he had been targeted for "suspicious activity."[72] Algabri was just one of many people with similar experiences.

- Under a program called "Project Lookout," the FBI circulated among corporations a list of hundreds of names of people whom it was seeking in connection with 9/11. The list, which was riddled with inaccuracies and contained the names of many people the Bureau simply wanted to talk to, was widely shared and re-shared, and quickly took on a life of its own. Companies began checking their customers against the list. The FBI admitted it had no way to remove innocent people from the list, because its distribution had spun beyond its control. No one knows how many innocent people have been denied jobs or suffered other harm because of the list.[73]

- Two giant health insurance companies, Blue Cross-Blue Shield of Michigan and Aetna, conducted a search through millions of customers' health insurance records for terrorists (none were found). The search of 6 million Michigan records by Blue Cross yielded 6,000 false positives, all of whom were "investigated further" by the company's employees. Aetna, which searched through 13 million records across the nation, refused to say how many false positives its search generated or how they were handled.[74]

- The government's "no-fly" lists of terrorist suspects have ensnared hundreds of innocent Americans who find themselves facing intense security scrutiny every time they try to fly, yet have no way of finding out how they got on a list, and no practical way to have their names removed.[75]

As such stories demonstrate, there are numerous problems with the government's watch lists:

- **Lack of due process.** Despite the bad effects that can accrue to those placed on such a list, there are no due process procedures that apply to those who are blacklisted, such as a right of appeal or a right to see the information upon which a listing is based. This violates the core American principle that no one should be punished without due process.

- **Slanted incentives.** There may well be strong bureaucratic incentives within the security agencies to place names on watch lists, and strong disincentives to remove names. After all, who would want to be the person responsible for removing or failing to add a name that later turned out to belong to a terrorist?[76]

- **Bloated lists.** Consistent with that dynamic, the U.S. government's watch lists appear to be ridiculously bloated; news reports have put the number of names in the millions.[77] That suggests it will become increasingly common for someone to be flagged based on such lists (especially when the inevitable cases of mistaken identification are added to the equation).

- **Private piggybacking.** There are no limits on the private uses or abuses of such lists, which are increasingly being used by landlords and even car dealers.[78]

An entire archipelago of government-enforced watch lists has been created haphazardly and without the carefully constructed checks and balances that such a powerful instrument demands. And now that system is being plugged in to the private sector, where a million eyes can watch for the millions of people on these lists.

Background checks: from reporting to enforcement

Watch list requirements are actually qualitatively different from other forms of outsourced surveillance. While many programs have increased the information flowing inward to the government, watch lists are a mechanism by which the government sends information outward into society. That serves two purposes:

A massive new infrastructure for everyday background checks in American life is being built.

- It alerts the government's information-collection networks to search for particular kinds of information, thereby increasing the power of the distributed surveillance system.

- It turns companies into sheriff's deputies, responsible not just for feeding information to the government, but for actually enforcing the government's wishes, for example by effectively blacklisting anyone who has been labeled as a suspect under the government's less-than-rigorous procedures for identifying risks.

A similar explosion of distributed enforcement/surveillance is taking place through the construction of a massive new infrastructure for everyday background checks in American life:

- Off-the-shelf software for conducting background checks is now being sold at Wal-Mart-owned "Sam's Club" stores for around $40. The software allows even the smallest business to carry out various checks by accessing databases compiled by the data aggregator Choicepoint.[79]

- Congress passed legislation called the PROTECT Act, which created a pilot program for FBI background checks on people who donate their time to various volunteer organizations. The FBI estimates that 26 million Americans a year could be required to be fingerprinted under this program. The criteria for failing one of these checks include the commission of any felony, or a misdemeanor involving controlled substances.[80]

- The Patriot Act required institution of checks on truck drivers with Hazmat licenses,[81] so the government is gearing up to do 3.5 million criminal background checks (which may actually be conducted by a private contractor such as Lockheed Martin). In a perfect example of public-private synergy, employers in the trucking industry may begin requiring all their drivers to get Hazmat licenses so they can get background checks on their drivers, whom they often don't trust.

- A growing normalization of background checks by employers of all kinds is emerging. One survey found 80 percent of companies now conduct background checks on job candidates.[82]

- The FBI's new Terrorist Screening Center plans to allow private-sector entities "such as operators of critical infrastructure facilities or organizers of large events" to submit lists of names to the government to be checked for "any nexus to terrorism."[83]

These checks are one of the fastest-growing areas of integration between the surveillance/enforcement functions of government and the private sector. There may well be good reasons for implementing background checks in certain circumstances, but an entire infrastructure for such checks is being constructed, and in the long run, there are few

areas of our lives that will be untouched. Few are stopping to ask what the consequences will be of, for example, banning people from driving a truck or volunteering in sports organizations because they have been busted for possession of marijuana, had a credit problem (real or erroneous) or angered a former landlord.

Enlistment in the government's surveillance web hurts business

The government has forced businesses to hire new staff and assume other expensive burdens to help conduct its surveillance. A wide variety of businesses, including even pawn shops, are faced with the prospect of setting up employee training programs, hiring compliance officers, creating written procedures, conducting annual "independent audits" or creating "customer identification programs."[84] Bank of America, for example, had to create a new department with six employees to handle the government's new surveillance mandates.[85] BellSouth employs a team of 16 full-time workers for the same purpose.[86] The brokerage industry alone will have to spend up to an estimated $700 million in the next few years complying with the Patriot Act.[87]

All these employees are, in effect, "outsourced" extensions of the government's growing surveillance machine, and these expenditures are hidden taxes that corporations often pass on to customers in the form of higher costs and fees.

Even worse for some companies is the fact that sweeping laws expanding government access to information could endanger overseas business deals. Canadians have recently expressed concern that because of the Patriot Act, their personal information could be placed in the hands of the FBI if contracts to perform outsourced functions for the Canadian government are given to U.S. companies.[88]

Failure to comply with the government's new mandates can also entail more direct costs; already one company, Western Union, has been fined $8 million under the Patriot Act for failing to report multiple "suspicious" transactions.[89]

The costs of airline passenger profiling

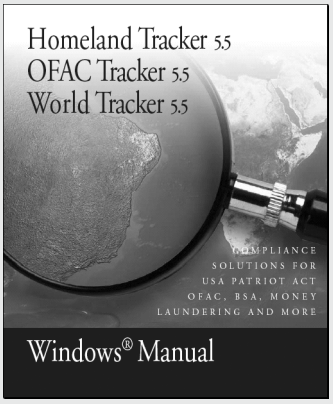
Perhaps the biggest example of burdensome surveillance mandates is the standardization of airline reservations and identity data that would be required by CAPPS II or other passenger-profiling schemes. The independent contractors that handle reservations for most airlines and the other computer systems to which they connect, from Web sites to travel agencies, are simply not equipped to routinely collect names, addresses and telephone numbers for all travelers. Many people travel

Sweeping laws expanding government access to information could endanger overseas business deals.

under group reservations, for example, in which a block of seats is reserved under just one name. And there is not even a field for date of birth in the existing databases – and it is no simple matter to add one.

The cost of rebuilding these interlocking systems to airlines, travel agents and the traveling public would be enormous; no systematic study has been done, not even by the government, but for CAPPS II, travel writer Edward Hasbrouck has estimated the cost at $1 billion,[90] and the International Air Transport Association reported estimates of more than $2 billion.[91] The TSA has never explained who will bear this expense or even sought to detail it. And of course that expenditure is only the beginning; there is also the cost to travelers in new hassles and frustrations.[92] The Association of Corporate Travel Executives testi-

Terrorist investigations in a box



An entire industry has sprung up to produce software that makes it easier for companies to enforce the government's blacklists and other mandates. An example is "Homeland Tracker," produced by a subsidiary of the giant database company Choicepoint to "help any business comply with OFAC and USA PATRIOT Act regulations." The manual proudly touts the software's ability to "get identity verification, check individual names, scan customer files" and "build personal accept and deny lists" (otherwise known as blacklists). Once a company's customer data is "scanned for violations against all data lists" – that is, government watch lists – the software lets the company "scan, block or reject business transactions" involving any entities "that threaten national security."[93]

This kind of product is offered by more than 50 companies and is being used, according to one survey, by 83 percent of financial companies for watch list screening, and by 50 percent to analyze transactions for money-laundering violations.[94]

fied that a "conservative estimate" of the cost of CAPPS II to business in delays and denied boardings would be $2 billion.[95]

By assuming the expenses of hiring workers, building new systems and procedures and purchasing software, businesses are helping to finance the creation of a legal and technological infrastructure for the systematic surveillance of individuals through their private-sector transactions. The government has always enlisted the help of citizens and others in fighting criminals, through such devices as "most wanted" posters. But that relatively simple device is worlds away from the wholesale recruitment of private corporations as extensions of the government's mass information-collecting apparatus.

Mass Data Use, Public and Private

Ultimately, the U.S. may need huge databases of commercial transactions that cover the world or certain areas outside the U.S.... Acxiom could build this mega-scale database.
– Doug Dyer of the Pentagon's Total Information Awareness program[96]

As we have seen, the government is recruiting both individuals and corporations into an emerging surveillance system. TIPS-like programs aim to promote and organize individuals' vigilance over each other, and feed the output of that mutual observation to the government. And, by plugging into the growing torrents of data swirling through private-sector computers, security agencies are doing the same thing with corporations: turning them into bigger, more far-reaching versions of the cable guy, able to inform on millions of customers in a single bound.

But the progression toward a surveillance society involves much more than efforts to gather information from particular organizations or even particular industries. It also includes efforts at the mass aggregation of information about individuals that aim to do for the rest of American life what the Patriot Act is already doing for the financial sector. If allowed to go far enough, this trend would turn America into a truly Orwellian society.

Data mining

A primary motivation for and justification of mass data gathering about Americans is a group of techniques loosely labeled "data mining." The idea behind data mining is to tap into the ever-growing number of databases containing details on individuals' behavior, aggregate that data to form rich pictures of individuals' activities and then use computer models to scrutinize them en masse for suspicious behavior.

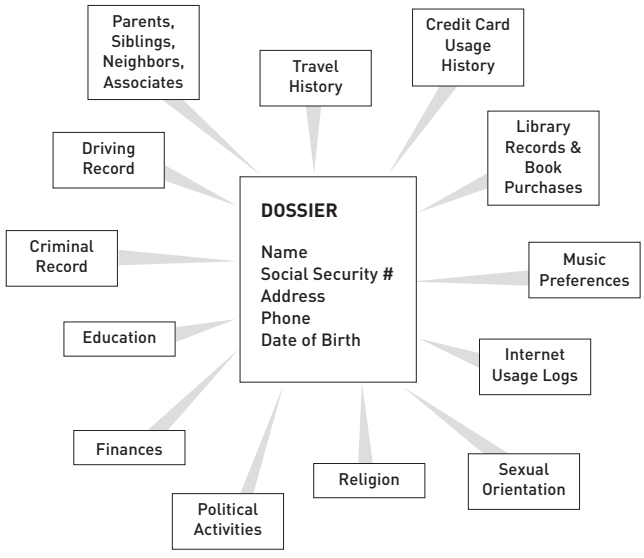
Interest in this concept within the government has sharply raised the stakes of government access to third-party data, because it takes scattered, disconnected databases that may be relatively harmless in isolation and transforms them into a means for the government to monitor individuals' activities.

While data mining has never been validated as a method for catching terrorists, it has been pursued by numerous government agencies, from the Army to NASA. The most notorious example is the Pentagon's now-defunct "Total Information Awareness" program, which sought to use data mining to help identify terrorists from among the hundreds of millions of innocent individuals in the United States.

From the start, TIA was premised on a tightly interlinked relationship between government and private-sector data companies. Program director John Poindexter of the Defense Advanced Research Projects Agency (DARPA) explained that the goal was to mine "the transaction space" in order to find "signatures" of terrorist activity. A graphic on the TIA Web site listed the types of databases that would make up this "transaction space," including financial, medical, travel, "place/event entry," transportation, housing and communications.

Interest in this concept within the government has sharply raised the stakes of government access to third-party data.

Private companies, of course, hold much of the data in these categories, and in order to achieve Poindexter's stated goal of weaving these databases together so that they can be treated "as if they were one centralized database," the government would clearly need to secure access to vast stores of private-sector data.



Total Information Awareness: far from unique

Congress ultimately voted to strip the funding from Poindexter's program. But TIA was hardly unique. Another program intended to aggregate and analyze vast amounts of private-sector information on the activities of Americans is the MATRIX, which stands for "Multi-State Antiterrorism Information Exchange." Like TIA, this program is based on bringing together vast amounts of information to detect terrorism and other crimes, except the MATRIX is run at the state level, and combines government databases from participating states with a private database that claims to have "20+ billion records from 100's of sources."[97]

Parts of the original TIA program live on in the Pentagon's secret "black budget."

At one time 16 states had agreed to participate in the MATRIX. But as a result of the public light thrown on the program by the media and by freedom of information requests filed by the ACLU, at least two-thirds of its members dropped out as of March 2004.[98]

The program continues, and in a move that is typical of the industry, Seisint is being purchased by LexisNexis, a giant data company, raising the prospect that even more torrents of information will be fed into the program.[99]

Other government data mining projects are also afoot:

- The NSA has a program called "Novel Intelligence From Massive Data," about which little is known.[100]
- The CIA reportedly is using a data-mining program called Quantum Leap that "enables an analyst to get quick access to all the information available – classified and unclassified – about virtually anyone." (The CIA's deputy chief information officer told a reporter that the technology is "so powerful it's scary" and "could be Big Brother.")[101]
- Parts of the original TIA program live on in the Pentagon's secret "black budget."
- A May 2004 survey of federal government data-mining efforts by the General Accounting Office revealed at least four data-mining programs that use personal information from private-sector databases in the hunt for terrorists. For example, the GAO identified a program run by the Defense Intelligence Agency that mines data "to identify foreign terrorists or U.S. citizens connected to foreign terrorism activities."[102]

Regardless of the activities of any particular government agency, it is clear that because of data mining, and the data aggregation that it depends upon, the compilation and sharing of information gathered by the private sector has assumed a much greater importance than in the past. It raises the prospect that information collected by one's broker, supermarket or catalog retailer will become data points in a frighteningly complete dossier, scrutinized by suspicious government security agencies.

Data aggregators are operating in a world where their work is becoming increasingly frightening and politically charged.

Data aggregators

Government agencies are not the only organizations that are interested in creating high-resolution pictures of individuals' activities by drawing together data from a variety of sources. Companies called "data aggregators" do the same thing for profit. These companies, which include Acxiom, Choicepoint, LexisNexis and many others, are largely invisible to the average person, but make up an enormous, multi-billion-dollar industry. The Privacy Act of 1974 banned the government from maintaining information on citizens who are not the targets of investigations – but law enforcement agencies are increasingly circumventing that requirement by simply purchasing information that has been collected by data aggregators.[103]

Originally fueled by the economic drive to make expensive corporate marketing campaigns more efficient, these companies are operating in a world where their work is becoming increasingly frightening and politically charged – in part because of the new post 9/11 environment and the government's corresponding hunger to gather as much data as it can, and in part because of their very success in gathering more and more information about everyone.

Data companies collect information from courthouses and other public sources, as well as marketing data – sometimes including extremely personal information, such as lists of individuals suffering from incontinence, prostate problems and clinical depression.[104] Some databases are even co-ops in which companies agree to contribute data about their own customers in return for the ability to pull out rich profiles of their customers based on the data contributed by all members. Once such company, Abacus Direct, for example, boasts to prospective members that their data will be "combined with other 1,700+

How data mining is used: a snapshot

The amount of information that is available about a person once you have his or her name and address is stunning. A marketing brochure published by the data company and credit rating giant Experian provides a snapshot of the kind of practices that have become common.

The brochure describes how Experian helped the electronics retailer Best Buy "develop a 360-degree view of their customers." Having gathered basic information about its customers from "19 customer touch-points," Best Buy "enhanced over 50 million customer records" with data compiled by Experian. That data came from "more than 3,500 public and proprietary data sources," and includes age, estimated income, occupation, "lifestyle data" and data about individual's product purchases "such as PC ownership and others."[105]

It is unclear whether Experian was allowed to keep the purchase records of Best Buy's customers as part of this deal. It is clear, however, that many companies are betraying their customers by sharing the details of their transactions with data companies that add them to the dossiers they maintain about us.

companies' transactions," that "Consumer buying behavior [is] defined for over 90 million households (90 percent of U.S.)," that they have records of 3.5 billion transactions and that – lest any corporate members fret over betraying the details of their customers' activities – "It's a confidential alliance."[106]

Government customers

As we have seen, all the information gathered by these companies is now easily available to government security agencies – whether through the many legal tools available to them for seizing personal information held by third parties like Experian, or by simply buying it. And the government is, in fact, buying information from these companies. One of the biggest data aggregators, for example, Choicepoint, claims to have contracts with at least 35 government agencies. It has an $8 million contract with the Justice Department that allows FBI agents to tap into the company's vast database of personal information on individuals, as well as contracts with the Drug Enforcement Administration, the U.S. Marshals Service, the IRS, the Bureau of Citizenship and Immigration Services (formerly INS) and the Bureau of Alcohol, Tobacco and Firearms.[107]Another data aggregator, Seisint Inc., has received more than $9.2 million in grant money from the Department of Justice and the Department of Homeland Security to provide commercial data to the MATRIX program.[108]

One of the biggest data aggregators claims to have contracts with at least 35 government agencies.

The government is not just dipping into a pre-existing commercial marketplace to purchase data; companies are actually creating and reshaping their products to meet the needs of government security agencies.[109] The fact is, private companies are increasingly moving in to perform functions that used to be carried out by the police.

Data companies provide information and services that include financial reports, education, professional credential and reference verification, felony checks, motor vehicle records, asset location services, and information on an individual's neighbors and family members, as well as the "location of witnesses, suspects, informants, criminals, [and] parolees" and the "verification of identity in criminal and civil investigations" and in "national security matters."[110] Tens of thousands of federal law enforcement agents have access to these services, with few safeguards against abuse.[111]

Not just federal agencies but also many local police departments subscribe to private-sector information services that can provide officers with information – such as a list of a person's past roommates – that would spark outrage if maintained directly by the police in their own files. In the newest twist, officers on the beat are even being given the power to access this kind of data on the fly using handheld wireless devices.[112]

Just as 19th century commercial file-keeping techniques began as a means of determining creditworthiness, and then were used to keep tabs on "Reds" and labor agitators,[113] so we are now witnessing the transmogrification of commercial databanks originally created for commercial purposes into security tools. And although these new tools are extremely powerful, they are constrained by few legal, procedural or technological safeguards against abuse.

The advantages of private surveillance

The use of private-sector data aggregators allows the government to insulate surveillance and information-handling practices from privacy laws or public scrutiny. That is sometimes an important motivation in outsourced surveillance. Private companies are free not only from complying with the Privacy Act, but from other checks and balances, such as the Freedom of Information Act. They are also insulated from oversight by Congress and are not subject to civil-service laws designed to ensure that government policymakers are not influenced by partisan politics; unlike federal government workers, private employees can make donations to political campaigns.[114]

Other examples of government officials nurturing surveillance schemes that rest in private hands include:

- **Minnesota's "Multiple Jurisdictional Network Organization."** In a case reminiscent of the mid-20th century private file-keeping groups, it emerged in 2003 that a private group, the Minnesota Chiefs of Police Association, was allowing the police to search its database of law enforcement case files from around the state. Raw case files contain not just criminal record information, but records of any interaction with the police, whether as victim, witness, gun-permit applicant or even the subject of an accusation by a disgruntled neighbor or coworker. The database has been shut down repeatedly because of privacy and security concerns, but may return as a purely state-owned and operated system.[115]

- **Image Data's "TrueID" system.** The Secret Service provided technical assistance and nearly $1.5 million in federal funds to a company attempting to compile a national database of driver's license photographs and make them available for security and commercial purposes. Under the scheme, individuals' photographs would pop up when they appeared at security checkpoints or used a credit card. The plan, which amounted to a privatized national ID system that security agencies would never have dared propose directly, collapsed after it provoked a public outcry.[116]

Pro-Surveillance Lobbying

'In 20 years, do you think the global database is going to exist, and will it be run by Oracle?' I asked. 'I do think it will exist, and I think it is going to be an Oracle database,' he replied. 'And we're going to track everything.'
– Jeffrey Rosen interview with Oracle CEO Larry Ellison[117]

As we have seen, there are many ways in which the government is pressuring corporations to do surveillance on its behalf. But the reverse is also true: Some corporations are pressuring the government to invest in surveillance.

Airport officials were receiving pitches from security technology companies within days of the 9/11 attacks.

Surveillance is big business. Because of the explosion of computers, database technology and information gathering, surveillance technologies are emerging as one of the ripest plums for companies to pluck in the new "anti-terrorism biz." E-mails obtained by the

ACLU (as part of its effort to monitor face-recognition technology) show that airport officials were receiving pitches from security technology companies within days of the 9/11 attacks.[118]

Enormous sums of money are being poured into government research and development on anti-terror initiatives – an estimated $115 billion in 2003 alone, rising to an estimated $130 billion to $180 billion a year through 2010.[119] And many companies want a piece of that action. Examples include:

- **Lockheed Martin.** The defense giant has received a five-year, $12.8 million contract to work on the CAPPS II airline profiling system. It also works on identification systems with the FBI and others and was a major recipient of contracts by Poindexter's office at DARPA.[120]

Defense contractors are turning their focus inward to applications involving surveillance within the nation's borders.

- **Acxiom.** The Arkansas data aggregator paid Gen. Wesley Clark $830,000 to help it obtain post-9/11 contracts. Clark lobbied Treasury Secretary Paul O'Neill and aides to FBI Director Robert Mueller, and even met personally with Vice President Dick Cheney.[121]

- **Choicepoint.** The Georgia data company increased its lobbying expenditures fourfold after 9/11, from $100,000 in 2000 to more than $400,000 in 2002.[122]

These companies are hardly alone; one 2003 study found that 569 companies had registered a homeland security lobbyist. As one lobbyist told *The New York Times*, "the major defense contractors want to move into the homeland security arena in a big way."[123] And often that means turning their focus inward from the development of fighter jets and other weapons designed for overseas combat to applications involving surveillance within the nation's borders.

It is not possible to determine the overall extent to which private-sector lobbying has actually driven the government's push for increased surveillance, as opposed to simply helping companies fight for pieces of a pre-determined government pie. It will be up to historians and investigative reporters to measure the role of companies pushing new software products, or seeking to develop a homeland security market for their pre-existing data stores. But in at least some cases, major new impetus for surveillance-friendly policies has clearly come from the private sector:

- **TIA.** The Pentagon's TIA program was proposed by a private company, an engineering services firm called Syntek. Syntek vice president John Poindexter worked on components of TIA for years before eventually becoming director of the DARPA's Information Awareness Office, which oversaw the program.[124]

- **The MATRIX.** The interstate MATRIX program similarly originated with a private company, the data aggregator Seisint. In 2001, the company's founder approached Florida police with the idea, and Seisint began developing the program for Florida, which was later joined by other interested states.[125]

- **National ID Cards.** Larry Ellison, the CEO of Oracle Software, almost single-handedly created a national debate over the notion of a U.S. national identity card in late 2001 by calling for such a card and promising to provide the software for it without charge. Critics noted that he did not agree to pay for the far more lucrative servicing contracts on the system.[126]

- **Face Recognition.** In the wake of 9/11, vendors of face-recognition software began to aggressively tout their product as a "nationwide shield" that would prevent future attacks, leading to the experimental deployment of the technology in airports around the nation. (Most quickly concluded that the technology was not up to the task.)[127]

Insufficient powers of surveillance was not America's problem on 9/11; a congressional investigation into the attacks as well as reports issued by the National Commission On Terrorist Attacks Upon The United States (the "9/11 Commission") found that the government's failure to prevent them was a result of fundamental organizational breakdowns in the intelligence community, and the government's failure to make effective use of the surveillance powers it already had.[128] But there is much more money to be made providing complex, cutting-edge technological solutions to security problems than there is in sorting out organizational or bureaucratic problems, or fixing problems with the basics of security by, for example, strengthening airplane cockpit doors or increasing the professionalism of airport security screeners.

The power of government and the power of corporations, instead of being set against each other, are actually becoming aligned.

It would be a double tragedy if the emerging surveillance-industrial complex were not only to lobby for increased surveillance on Americans, but also to divert resources from security measures that would be far more likely to be effective in protecting Americans from attacks.

Six Conclusions

We should take nothing for granted.
– President Eisenhower

Conclusion #1: An alliance of unchecked interests

Individual freedom is always at risk in the face of large, powerful institutions. In America, this problem has been addressed by setting power against power. In the case of government power, that has been accomplished through the system of checks and balances put in place in our Constitution. In the case of corporate power, that has been accomplished through competition, which sets company against company, and through regulation, which sets the power of government against the power of corporations (including the government's antitrust powers, to ensure that company remains set against company).

In the area of privacy, however, these time-tested protective arrangements are increasingly breaking down:

- **Insufficient and eroding checks on government.** The checks and balances that are supposed to restrain government power are not being put in place, as shown by the lack of due process protections for watch lists, for example, or rules to handle data collected from citizen tip lines. Often, this is because of the rapidity with which new information technologies have emerged – but existing checks and balances are also being weakened, such as judicial oversight of surveillance, which was reduced sharply by the Patriot Act.

- **Insufficient checks on corporations.** The virtual absence of governmental reg-

ulation of corporate privacy in the U.S. – unique in the developed world – gives companies a free hand to sell, trade and share the details of their customers' transactions without their permission or knowledge. And while competitive forces may limit data sharing among some companies, the thriving marketplace of data brokers often serves the function of bridging that gap.

Sifting through the lives of hundreds of millions of people is an inefficient, highly unreliable means of discovering a one-in-a-billion terrorist.

The power of government and the power of corporations, instead of being set against each other, are actually becoming aligned. There are certainly companies and industries concerned about privacy, and others concerned about the costs of complying with the new surveillance mandates. But most companies have a strong incentive to maximize consumer data collection, and even the most privacy-protective company is helpless in the face of official demands for customer information. Other companies, as we have seen, actively lobby for wider government use of personal records.

The United States has experienced occasional periods of intense social and political conflict, such as the Vietnam War, the Civil Rights movement and the labor movement earlier in the 20th century. Given the greatly enhanced surveillance powers of major corporations and government security agencies, which in the past have actively opposed such movements, how will the forces fighting for change fare today and the next time such a period emerges?

The kinds of activities and information that the Founding Fathers sought to protect through the Fourth Amendment have moved out of the home in modern life.

Conclusion #2: Mass surveillance threatens freedom more than it threatens terrorists

The government's post-9/11 efforts to vacuum up and sift through masses of private-sector data is premised on the impulse that "if we had just known who those people were and what they were doing, we could have stopped them – so let's track everyone." The tragedy is that mass surveillance is not only dangerous to our liberties, but is unlikely to be effective. Sifting through the lives of hundreds of millions of people is an inefficient, highly unreliable means of discovering a one-in-a-billion terrorist. The best way to stop terrorism is still through old-fashioned intelligence and law enforcement techniques that rely on working outward from known leads and suspects. Attempting to work inward from the entire resident and visitor population of the United States to locate a handful of terrorists will harm many innocent people yet leave us vulnerable.

Working outward from known leads is not only more effective, but is also compatible with an entire body of law that has grown up over hundreds of years to prevent abuses by all-too-human investigators. The drive to detect wrongdoing through the mass scrutiny of individual records from the private sector, on the other hand, would violate a principle that is core to our legal system: The government cannot invade your privacy unless it has individualized reason to believe that you are involved in wrongdoing. The principle of individualized suspicion not only protects individuals against unfair treatment, but also imposes a necessary discipline on police investigators, who can be tempted at times to engage in wasteful and inefficient fishing expeditions. Unfortunately, as this report demonstrates, the fishing expedition

approach is rapidly being hardwired into our laws and even our technologies.

Conclusion #3: The courts must catch up

Historically, the courts have been slow to adapt the Fourth Amendment[129] to new technology, and today is no different. When the telephone came into use, the Supreme Court failed to give legal protection to the content of telephone conversations against government wiretapping, instead engaging in literal-minded hairsplitting about whether particular eavesdropping devices physically penetrated a "constitutionally protected area." It was almost 40 years before the Supreme Court finally ruled that a wiretap, just like a physical search, required a warrant based on probable cause, and that "the Fourth Amendment protects people, not places."[130]

Today, the Supreme Court has still not recognized the right to privacy in highly personal information held by third parties – whether financial records, medical records or library and book records – on the theory that there can be no "reasonable expectation" of privacy regarding such information. When the Constitution was written, the home was the center of economic, financial and even medical life, and personal records and writings were likely to be stored there, not on the servers of a multinational corporation. The Founders therefore created strong protections for people's "houses and effects."

Today our homes remain highly protected from government scrutiny, but the kinds of activities and information that the Founding Fathers sought to protect through the Fourth Amendment have moved outward due to computers, telecommunications and other developments of modern life. But though privacy in one's affairs is no less necessary today, we are now exposed to easy scrutiny by the government and other powerful institutions.

As with phone calls last century, so with third-party records today: The Court has yet to transcend the particular, 18th century formulation of privacy written into the Constitution and embrace the deeper ethos of privacy that the Founders intended to protect, and that is necessary to preserving a healthy democracy in an age of high technology.

Our laws will probably catch up, as they did with the telephone, but we must ensure that they are given the chance. It is a very real danger that, given the time it takes the courts to adjust to new technology, our law enforcement and national security establishments will take advantage of the lag to institutionalize data mining and other surveillance practices that would never be accepted otherwise.

Conclusion #4: The ACLU is leading the fight

The ACLU is working hard across many of the dimensions described in this report to combat the emergence of a public-private surveillance state. In the past two years, the ACLU:

- **Helped defeat TIPS.** The ACLU led public opposition to this intrusive proposal, both in the media and in the halls of Congress. (See www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11295&c=206).

- **Helped defeat TIA.** The ACLU was instrumental in creating and maintaining public pressure on this program, leading to its eventual defeat by Congress. (See www.aclu.org/Privacy/Privacy.cfm?ID=14729&c=130).

Today the fight continues. The ACLU is:

- **Fighting against racial profiling.** A broad assault on the kind of racial profiling implicitly encouraged by TIPS-like "terrorism watch" programs has been one of the

ACLU's highest priorities both before and after 9/11. (See www.aclu.org/profiling).

- **Fighting the MATRIX.** By coordinating action among the ACLU's state affiliates, including the filing of state open-records requests and efforts to inform state legislators about the program, the ACLU has helped reduce the number of participating states by two-thirds. (See www.aclu.org/matrix).

- **Fighting CAPPS II.** From media appearances to public testimony to generating citizen faxes to lobbying in the halls of Congress and the European Union headquarters in Brussels, the ACLU has helped point out the flaws of this unnecessary program and, so far, delay its deployment. (See www.aclu.org/capps).

- **Working to discover how the government's secret watch lists operate.** The ACLU has filed a lawsuit to force the government to comply with a Freedom of Information Act (FOIA) request seeking information on how the government's No-Fly list operates and how individuals can get off it. (See www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15422&c=206).

- **Challenging the No-Fly list in court.** In addition to seeking information, the ACLU has also directly challenged the No-Fly list through a class action lawsuit filed on behalf of innocent people caught up by the list. (See www.aclu.org/nofly).

- **Fighting in court to find out how the Patriot Act is being implemented.** The ACLU has filed a lawsuit to force the government to comply with a FOIA request for information on how often it has used the Patriot Act to obtain individuals' records from businesses or other third parties. (See www.aclu.org/patriotfoia).

- **Challenging the Patriot Act's "business records" section in court.** The ACLU has launched a direct legal challenge to Section 215 of the Patriot Act, which greatly expands the government's ability to secretly obtain data held by libraries, businesses and other third parties. (See www.aclu.org/section215).

- **Challenging the use of "National Security Letters" in court.** The ACLU has also filed a direct legal challenge to the Patriot Act's dramatic expansion of law enforcement's authority to use National Security Letters to demand customer records without judicial oversight. (See www.aclu.org/nsl).

- **Working in Congress to reverse the worst provisions of the Patriot Act.** ACLU lobbyists have been working in Congress to pass legislation called the SAFE Act. (See www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15962&c=206).

- **Running a national grassroots campaign to build opposition to Patriot Act surveillance.** With a full-time team of community organizers, the ACLU has helped hundreds of communities, representing nearly 20% of the U.S. population, to pass resolutions in opposition to the Patriot Act. (See www.aclu.org/resolutions).

- **Exposing government and private-sector surveillance.** The ACLU has produced numerous reports to inform the public and the news media about government surveillance. They include:

  - "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society" (www.aclu.org/monster)

  - "Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and

Personal Belongings Without Telling You" (www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13246&c=206)

- "The Dangers of Domestic Spying by Federal Law Enforcement: A Case Study on FBI Surveillance of Martin Luther King" (www.aclu.org/Files/OpenFile.cfm?id=9999).

- **Working to discover how information has been shared by airlines.** The ACLU has filed FOIA requests with DHS and the TSA seeking information about how personal travel information from JetBlue and American Airlines was shared and used. (See www.aclu.org/jetblue).

- **Fighting expansion of CALEA.** The ACLU is working to prevent the expansion of CALEA, which would force Internet telephony companies to design their software to enable government eavesdropping. (See www.aclu.org/Privacy/Privacy.cfm?ID=15468&c=130).

Conclusion #5: Individuals must act to stem the supply of personal data

The government's strategy of relying on private-sector surrogates is a new and challenging development in the growth of surveillance. In the ACLU's view, the U.S. should emulate much of the rest of the developed world and create overarching data privacy laws that cover at least our most sensitive data, including data in the hands of the private sector. The United States is virtually alone among major industrialized nations in lacking such a law (or a federal privacy official charged with protecting the public).

But regardless of one's opinions about how the government should regulate the commercial sector, nearly everyone who cares about his or her personal privacy agrees that the government's use of the private sector to supply it with our personal information needs to be brought under control. One thing that consumers can do is to vote with their feet and their pocketbooks when they don't like what companies are doing behind their backs. In the short term, Americans must weigh in against the government's practice of "outsourcing surveillance" and make use of their role as consumers, shareholders and activists to put pressure on companies that are voluntarily participating in this emerging system.

The ACLU is creating a Web site to help individuals contact companies about their privacy practices: www.aclu.org/privatize.

Conclusion #6: We should take nothing for granted

In his Farewell Address of January 17, 1961, President Eisenhower famously warned that the "conjunction of an immense military establishment and a large arms industry is new in the American experience." We might update his words to describe what we are facing today: "the conjunction of an immense *security* establishment and a large *data* industry." Eisenhower's conclusion about what he dubbed the "military-industrial complex" was that:

> The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted.[131]

This warning applies just as strongly to the "surveillance-industrial complex" that is emerging in our own time. And the consequences of ignoring it would be just as dire.

ENDNOTES

[1] See Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society," ACLU, January 2003; online at http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39.

[2] Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System* (New York: Alfred A. Knopf, 1980), chapter 12.

[3] Operation TIPS Web pages from July 16 and August 8, 2002; available online at http://www.thememoryhole.org/policestate/tips-changes.htm.

[4] According to the 2000 census, the population of the 10 largest cities in the U.S. totaled 23,899,236. By recruiting 1 million participants from that population, TIPS would have turned one in every 24 residents of those cities into informants (and the proportion would be even higher if any smaller cities were included in the pilot program).

[5] Sandra Sobieraj, "Bush Urges Americans to Volunteer," Associated Press, January 30, 2002; available online at http://www.firehouse.com/news/2002/1/30_APbushvol.html.

[6] Citizen Corps, "Citizen Corps: A Guide for Local Officials," April 2002, p. 25; online at http://www.citizencorps.gov/pdf/council.pdf.

[7] Citizen Corps Councils home page at http://www.citizencorps.gov/councils/.

[8] "Coastal Beacon Program Continues," Coast Guard press release, July 17, 2002; online at http://www.uscg.mil/d1/newengland/press_releases/081-02.htm.

[9] "President Promotes Citizen Corps for Safer Communities," White House Press Release, April 8, 2002; online at http://www.whitehouse.gov/news/releases/2002/04/20020408-4.html.

[10] Eyes on the Water program Web page at http://www.uscg.mil/d9/eyesonthewater/howdoihelp.htm; Paul Singer, "Coast Guard asks help watching out for terrorism on Great Lakes," Associated Press, July 25, 2002; River Watch Web page at http://www.michigan.gov/msp/0,1607,7-123-1589_3492-73050--,00.html. The primary difference between these programs and TIPS appears to be that while TIPS would have been centralized, now every Coast Guard district is setting up its own program.

[11] "Highway Watch Fact Sheet," Highway Watch home page; online at http://www.highwaywatch.com/aboutus/fsheet.html. Like some of the coastal watch programs, Highway Watch was listed as an "existing system" on an "Operation TIPS Fact Sheet" published by Citizen Corps, but continues to operate despite Congress's decision to shut down TIPS. Citizen Corps Web site, "Operation TIPS Fact Sheet," undated. The fact sheet was removed from the government's Web site after TIPS was cancelled, but is available online at http://www.thememoryhole.org/policestate/last-tips.mht. See also Alice Lipowicz, 'Highway Watch' Truckers Are the Eyes and the Ears of "Homeland Security," *Congressional Quarterly Homeland Security*, June 8, 2004.

[12] CAT Eyes, "About Us," and "The Program: Neighborhood Block Watch Duties Using CAT Eyes," available at http://www.cateyesprogram.com. The program places a commendable emphasis on teaching trainees not to use race as a basis for suspicion.

[13] Jennifer Steiner, "Anderson Township Sheriff's Department Recruits Realtors," WCPO 9News, July 8, 2004; online at http://www.wcpo.com/news/2004/local/07/07/realtors.html. Jennifer Edwards, "Realty agents, sheriff team up," *Cincinnati Enquirer,* July 20, 2004; online at http://www.enquirer.com/editions/2004/07/20/loc_loc4and.html.

[14] Brian Baskin, "Workers recruited in war on terror," *Orlando Sentinel*, July 8, 20042004; online at http://www.orlandosentinel.com/news/local/orange/orl-aseccap08070804jul08,1,152972.story. Baskin, "'Aware' primer will be revised," *Orlando Sentinel,* July 16, 2004; online at http://www.sun-sentinel.com/news/local/southflorida/orl-loccapfolo16071604jul16,0,4840672.story.

[15] "Governor Pataki Announces Public Security Tips Hotline," press release, Office of the Governor, New York State, Sept. 16, 2002; online at http://www.state.ny.us/governor/press/year02/sept16_1_02.htm. See also Nat Hentoff, "Ashcroft's Shadowy Disciple: Someone to Watch Over Us," *Village Voice*, November 15th, 2002.

[16] Air Force Office of Special Investigations, Eagle Eyes home page at http://www.dtic.mil/afosi/eagle/index.html.

[17] Brian McWilliams, "DoD Logging Unverified Tips," *Wired News*, June 25, 2003; online at http://www.wired.com/news/politics/0,1283,59365,00.html.

[18] See description of JetBlue case, p. 10. William M. Arkin, "Mission Creep Hits Home: American armed forces are assuming major new domestic policing and surveillance roles," *Los Angeles Times*, November 23, 2003.

[19] Quote is a link on Louisiana Homeland Security page at http://www.loep.state.la.us/homeland/hls-main-citizens.htm. Clicking on the link brings readers to the federal Citizen Corps homepage.

[20] Maryland Joint Terrorism Task Force Flyer, "Maryland Law Enforcement Seeks Your Help in Preventing Terrorism!"; online at http://baltimore.fbi.gov/mdjttfflyer1.pdf.

[21] "Regional Terrorism Task Force Advises Public On 'Threat Level Orange' Protections," press release, Lucas County, Ohioassuming Web site, May 29, 2003; online at http://www.co.lucas.oh.us/HomelandSecurity/Stories/OrangeLevelProtectiveMeasures.asp.

[22] Christopher Tripp, "Flashing highway signs proliferate, but do they help?" (Fredericksburg, VA) *Free Lance-Star*, May 11, 2003; online at http://www.freelancestar.com/News/FLS/2003/052003/05112003/970175.

[23] Example online at http://www.state.oh.us/odps/homelandsecurity/homeresponseguidefamilies.pdf. The warning applies to all alert levels except the lowest – a status unlikely to be declared anytime in the foreseeable future.

[24] National Crime Prevention Council, "United for a Stronger America: Citizens' Preparedness Guide," pp. 2, 6, 20; online at http://www.citizencorps.gov/pdf/cpg.pdf. This advice is reminiscent of Federal Civil Defense public-service films of the 1950s, which were long on frightening facts about possible attacks, and short on advice for citizens likely to be useful in case of attack. See for example, "What You Should Know About Biological Warfare," Federal Civil Defense Administration public-service film, 19521952; available online at http://www.archive.org/movies/details-db.php?collection=prelinger&collectionid=01449. This film explains in frightening detail the nature of the threat (reinforced by a soundtrack of scary music), and contains only vague suggestions for what to do about it, such as "keep yourself clean." The film's main message: "cooperate with the authorities!"

[25] U.S. Coast Guard, Marine Safety Office Pittsburgh; online at http://www.uscg.mil/d8/mso/pittsburgh/PittsburghBrochure.pdf.

[26] Frank James, "Terror tip lines prone to stereotyping," *Chicago Tribune*, April 17, 2003; available online at http://www.sanluisobispo.com/mld/sanluisobispo/news/politics/5664237.htm. Dan Fesperman, "Md. Tip center a model for U.S. security," *Baltimore Sun*, Jan. 12, 2004.

[27] Privacy Act of 1974, PL 93-579, Sec. 3, Dec. 31, 1974, 88 Stat. 1897. The privacy act does apply to subcontractors who are directly performing the government's work for it, but not companies that collect data for their own reasons.

[28] "Report to the Standing Committee on Governmental Operations of the New York State Assembly," June 8, 1976, cited in Ross Gelbspan, *Break-Ins, Death Threats and the FBI: The Covert War Against the Central America Movement* (Boston: South End Press, 1991), 80-81.

[29] Gelbspan, pp. 45, 77-84, 169-172. The LAPD files were the subject of a 1983 lawsuit filed by the ACLU on behalf of many of the victims of police spying, which eventually resulted in a $1.8 million settlement from the city of Los Angeles.

[30] Donner, 417-419.

[31] James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War Through the Dawn of a New Century* (New York: Doubleday, 2001), 434.

[32] James Bamford, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency* (Boston: Houghton Mifflin Co., 1982), 236-50. Operation Shamrock was not shut down until 1975. However, L. Britt Snider, who had investigated Operation Shamrock for the Church Committee in 1975 (and later became inspector general of the CIA), observed that "relations between intelligence agencies and the private sector endured." Bamford, *Body of Secrets*, 440.

[33] Bamford, *Puzzle Palace*, 244-45, 248-52.

[34] See Stanley and Steinhardt, "Bigger Monster," 4.

[35] Ryan Singel, "JetBlue Shared Passenger Data," Wired News, Sept. 18, 20032003; online at http://www.wired.com/news/privacy/0,1848,60489,00.html. Ryan Singel and Noah Shachtman, "Army Admits Using JetBlue Data," *Wired News*, Sept. 23, 2003; http://www.wired.com/news/privacy/0,1848,60540,00.html.

[36] Electronic Privacy Information Center, "Northwest Airlines Gave NASA Personal Info on Millions of Passengers; Disclosure Violated Privacy Policy," press release, Jan. 18, 2004; online at http://www.epic.org/privacy/airtravel/nasa/pr1.18.04.html. See also Sara Kehaulani Goo, "Northwest Gave U.S. Data on Passengers," *Washington Post*, Jan. 18, 2004; online at http://www.washingtonpost.com/wp-dyn/articles/A26422-2004Jan17.html.

[37] "American Released Passenger Data," Associated Press, April 10, 2004; available online at http://www.wired.com/news/privacy/0,1848,63018,00.html.

[38] John Schwartz and Micheline Maynard, "F.B.I. Got Records on Air Travelers," *New York Times*, May 1, 2004; online at http://www.nytimes.com/2004/05/01/politics/01AIRL.html.

[39] Eunice Moscoso, "Feds demanding more info about companies' customers," *Atlanta Journal Constitution*, August 17, 2003; available online at http://www.ajc.com/business/content/business/0803/17patriot.html.

[40] Patrick Healy, "Colleges giving probers data on foreign students' finances," *Boston Globe*, Oct. 3, 2001. American Association of Collegiate Registrars and Admissions Officers, "Preliminary Results of the AACRAO Survey on Campus Consequences of the September 11 Attacks," October 4, 2001; online at http://www.aacrao.org/transcript/index.cfm?fuseaction=show_view&doc_id=434.

[41] Stephanie Stoughton, "Poll: Firms Relaxed Privacy Rules," *Boston Globe*, Oct. 8, 2001.

[42] InfraGard Web site at http://www.infragard.net/. See also http://www.govjobs.com/Cont/InfraGard/Infragard%20Secure%20Access%20Agreement.pdf.

[43] Chris Seper, "Combating Cybercrime: Different companies work together in groups organized by FBI," *Cleveland Plain Dealer*, Nov. 4, 2002; available online at http://www.infragard.net/library/ig_promotes_awareness.htm.

[44] *Cleveland Plain Dealer*, Nov. 4, 2002, op. cit. Two FBI agents in the Cleveland office denied such an arrangement. But the newspaper cites the chairwoman of the InfraGard national executive board: "I have the list with me," she told the paper.

[45] For a useful overview see Jim Dempsey and Lara Flint, "Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data," Center for Democracy and Technology, May 28, 2003; online at http://www.cdt.org/security/usapatriot/030528cdt.pdf.

[46] See Ann Beeson and Jameel Jaffer, "Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You," ACLU Report, July 20032003; online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13246&c=206. See also http://www.aclu.org/patriot.

[47] The only requirement is that the National Security Letter be "relevant to" an ongoing investigation. The ACLU has filed a lawsuit challenging the constitutionality of NSLs; see http://www.aclu.org/nsl.

[48] Intelligence Authorization Act for Fiscal Year 2004, P.L. 108-177, December 13, 2003, 117 Stat. 2599. See also Kim Zetter, "Bush Grabs New Power For FBI," *Wired News*, January 6, 2004; online at http://www.wired.com/news/privacy/0,1848,61792,00.html.

[49] In re Sealed Case, 310 F.3d 717, 746 (Foreign Intelligence Surveillance Court of Review 2002).

[50] Eunice Moscoso, "Feds demanding more info about companies' customers," *Atlanta Journal Constitution*, August 17, 2003; available online at http://www.ajc.com/business/content/business/0803/17patriot.html.

[51] Rod Smith, "Sources: FBI gathered visitor information only in Las Vegas," *Las Vegas Review Journal*, January 7, 2004; online at http://www.reviewjournal.com/lvrj_home/2004/Jan-07-Wed-2004/news/22934251.html. "Surveillance City," editorial, *Las Vegas Review-Journal*, Jan. 11, 2004; online at http://www.reviewjournal.com/lvrj_home/2004/Jan-11-Sun-2004/opinion/22961926.html.

[52] "Transactional Records NSLs Since 10/26/2001," available online at http://www.aclu.org/patriot_foia/foia3.html. See also Dan Eggen and Robert O'Harrow Jr., "US Steps Up Secret Surveillance: FBI, Justice Dept. Increase Use of Wiretaps, Records Searches," Washington Post, March 24, 2003; online at http://www.washingtonpost.com/ac2/wp-dyn/A16287-2003Mar23.

[53] Associated Press, "Net Effect: Antiterror Eavesdropping: Privacy Advocates Worry Civil Rights May be Trampled," May 27, 2002; available online at http://tinyurl.com/xmai.

[54] *Atlanta Journal Constitution*, August 17, 2003, op. cit.

[55] Miles Benson, "In the Name of Homeland Security, Telecom Firms Are Deluged With Subpoenas," Newhouse News Service, April 10, 2002; online at http://www.newhouse.com/archive/story1a041002.html.

[56] Stewart Baker, former General Counsel of the NSA, quoted in ibid.

[57] U.S. Department of Justice, "Joint Petition For Expedited Rulemaking," March 10, 2004; available online at http://www.steptoe.com/publications/FBI_Petition_for_Rulemaking_on_CALEA.pdf. Declan McCullagh and Ben Charmy, "FBI adds to wiretap wish list," CNET News, March 12, 20042004; online at http://news.com.com/2100-1028-5172948.html. Declan McCullagh, "Inside Cisco's Eavesdropping Apparatus," CNET News, April 21, 2003, online at http://news.com.com/2010-1071-997528.html.

[58] Kevin Poulsen, "Cyber Security Plan Contemplates U.S. Data Retention Law," SecurityFocus, June 18, 2002. The report, which was based on unnamed sources, was denied by the White House.

[59] Letter from James J. Foster, U.S. Mission to the EU (transmitting President Bush's proposal), to Romano Prodi, President of the European Commission, October 16, 2001, online at http://www.statewatch.org/news/2001/nov/06Ausalet.htm.

[60] "Majority of governments introducing data retention of communications," Statewatch, January 12, 2003, online at http://www.statewatch.org/news/2003/jan/12eudatret.htm.

[61] See Edward Hasbrouck, "What's wrong with CAPPS-II?"; online at http://hasbrouck.org/articles/CAPPS-II.html.

[62] Over the long run, the CRSs may reap significant financial benefits from selling the enhanced travel data they will be collecting, but the cost of collecting that data is still likely to be passed on to consumers (see p. 21).

[63] Cynthia L. Webb, "Uncle Sam Mothballs Screening Program," WashingtonPost.com, July 16, 2004; online at http://www.washingtonpost.com/wp-dyn/articles/A54487-2004Jul16.html.

[64] Richard Spillenkothen, Federal Reserve Board, "Testimony Before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate," January 29, 2002; online at http://www.federalreserve.gov/boarddocs/testimony/2002/20020129/default.htm.

[65] The USA-Patriot Act, P.L. 107-56, Section 365, 115 Stat. 272 (Oct. 26, 2001). Scott Bernard Nelson, "Patriot Act would make watchdogs of firms," *Boston Globe*, November 18, 2001.

[66] Inflation figures calculated using the historical inflation calculator at http://www.inflationdata.com.

[67] Quoted in Nelson, op. cit.

[68] "Financial Crimes Enforcement Network; Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity: Final Rule," 67 Federal Register, 60,579 (Sept. 26, 2002); the regulations stem from section 314 of the Patriot Act. Michael Isikoff, "Show Me the Money: Patriot Act helps the Feds in cases with no tie to terror," *Newsweek*, Dec. 1, 2003, online at http://www.msnbc.com/news/997054.asp.

[69] The rules do prohibit banks from disclosing the names to others, but they can themselves use them in "determining whether to establish or maintain an account, or to engage in a transaction." 67 Federal Register, 60,579, 60,586 (Sept. 26, 2002).

[70] "Transactions and Customer Identification Programs; Final Rules and Proposed Rule," Federal Register, 25089 (May 5, 2003). See also Kathleen Pender, "Would-be investor runs afoul of Patriot Act," *San Francisco Chronicle*, August 28, 2003; online at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/08/28/BU298595.DTL. *Portland Press Herald*, "Banks tighten rules on proving identity," *Portland Press Herald*, Sept. 22, 2003.

[71] Brian Braiker, "The 'Patriot' Search," *Newsweek Online*, June 3, 2004; online at http://msnbc.msn.com/id/5131685/site/newsweek.

[72] Sara B. Miller, "Blacklisted by the bank," *Christian Science Monitor*, August 25, 2003; online at http://www.csmonitor.com/2003/0825/p15s01-wmcn.html.

[73] Ann Davis, "Far Afield: FBI's Post-Sept. 11 'Watch List' Mutates, Acquires Life of Its Own," *Wall Street Journal*, Nov. 19, 2002.

[74] Amy Lee, "Blues, Aetna help hunt terrorists: Client, worker files checked against fed list," *Detroit News*, Nov. 16, 2003; "Insurance Giants Search for Terrorists," Associated Press, Nov. 17, 2003.

[75] The ACLU has filed a lawsuit on behalf of individuals victimized by these inaccurate lists. See http://www.aclu.org/nofly.

[76] Bruce Schneier, CRYPTO-GRAM newsletter, April 15, 2003; online at http://www.schneier.com/crypto-gram-0304.html. See also Schneier, Beyond Fear (New York: Copernicus Books, 2003), chapter 3.

[77] James Gordon Meek, "13 Million on Terror Watch List," *New York Daily News*, April 8, 2003; online at http://www.nydailynews.com/04-08-2003/news/wn_report/story/73628p-68132c.html. Tom Godfrey, "5 million on [U.S.] terrorism list," *Toronto Sun*, January 20, 2004; online at http://www.canoe.ca/NewsStand/TorontoSun/News/2004/01/20/318488.html.

[78] Dennis Hevesi, "When the Credit Check Is Only the Start," *New York Times*, October 12, 2003; online at http://query.nytimes.com/gst/fullpage.html?res=9C07E0D8163FF931A25753C1A9659C8B63. Douglas Hanks III, "Credit bureaus screening for terrorists," *Miami Herald*, July 6, 2003; online at http://www.miami.com/mld/miamiherald/6231536.htm.

[79] Adam Geller, "High-Tech Background Checks Hit Stores," Associated Press, March 8, 2004; available online at http://seattlepi.nwsource.com/business/aptech_story.asp?category=1700&slug=Background%20Check.

[80] PROTECT Act, P.L. 108-21, Section 108 (April 30, 2003); FBI presentation delivered at meeting of National Crime and Prevention and Privacy Compact Council, Alexandria, Virginia, October 3, 2003.

[81] The USA-Patriot Act, Section 1012, P.L. 107-56, 115 Stat. 272 (Oct. 26, 2001).

[82] Geller, op cit.

[83] Donna A. Bucella, Director, FBI Terrorist Screening Center, "Statement Before The House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, and the House Select Committee on Homeland Security, Subcommittee On Intelligence and Counterterrorism," March 25, 20042004; online at http://www.fbi.gov/congress/congress04/bucella032504.htm. See also Guy Taylor, "FBI up for private screens," *Washington Times*, March 26, 2004; online at http://www.washtimes.com/national/20040326-124121-1245r.htm.

[84] Caitlin Harrington, "Even Pawn Shops Feel the Hand of the Patriot Act," *Congressional Quarterly*, March 2, 2004.

[85] Meredith Jordan, "Banks Bracing for Effects of USA Patriot Act," *Atlanta Business Chronicle*, November 8, 2002.

[86] *AJC*, August 17, 2003.

[87] Lucas Mearian, "Brokerages face big IT bills to comply with USA Patriot Act," *ComputerWorld*, March 17, 2003.

[88] Judith Lavoie, "Canada risks U.S. privacy invasion: Canadians' personal information could be put in the hands of the FBI under American Patriot Act," *Times Colonist* (Victoria), March 4, 2004.

[89] New York State Banking Department, "Banking Department Fines Western Union $8 Million for Violating Bank Secrecy, USA Patriot, New York Banking Laws," press release and consent agreement, Dec. 18, 2002; online at http://www.banking.state.ny.us/pr021218.htm.

[90] Edward Hasbrouck, "Comments Re: Docket Number DHS/TSA-2003-1, 'Passenger and Aviation Security Screening Records'" ; online at http://hasbrouck.org/articles/Hasbrouck_TSA_comments-30SEP2003.pdf. See also Hasbrouck, "Why CAPPS-II would cost a billion dollars," blog entry, February 13, 2004; online at http://hasbrouck.org/blog/archives/000149.html.

[91] International Air Transport Association, "Airline Reservation System and Passenger Name Record (PNR) Access by States," March 15, 2004, p. 3; online at http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf.

[92] See General Accounting Office, "Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges," GAO-04-385, February 2004; online at http://www.gao.gov/new.items/d04385.pdf.

[93] Bridger Systems, Inc., "Homeland Tracker 5.5, OFAC Tracker 5.5, World Tracker 5.5: Windows Manual," 2003; online at http://www.bridgertracker.com/Downloads/WindowsManual55.pdf.

[94] Eunice Moscoso, "Feds demanding more info about companies' customers," *Atlanta Journal Constitution*, August 17, 2003available online at http://www.ajc.com/business/content/business/0803/17patriot.html. Deloitte & Touche

LLP, Anti-Money Laundering Compliance Survey, October 10, 2003 at 2. Available at http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_AMLComplianceSurvey_101003.pdf.

[95] Nancy Holtzman, Association of Corporate Travel Executives, testimony before the Subcommittee on Aviation of the House Transportation and Infrastructure Committee," March 15, 2004; online at http://www.acte.org/resources/press_release/testimony_to_congress.shtml.

[96] "Recommendations on Acxiom," e-mail from Doug Dyer to John Poindexter and Robert Popp, all of DARPA, May 21, 2002 (obtained through a Freedom of Information Act Request by the Electronic Privacy Information Center [EPIC]); , available online at http://www.epic.org/privacy/profiling/tia/darpaacxiom.pdf.

[97] Seisint, Inc., "Matrix Michigan Briefing," May 8, 2003, slide entitled "Seisint's Core Capabilities" (document obtained through open-records requests filed by ACLU).

[98] John Schwartz, "Privacy Fears Erode Support for a Network to Fight Crime," *New York Times*, March 15, 2004; online at http://www.nytimes.com/2004/03/15/technology/15matrix.html.

[99] Robert O'Harrow Jr., "LexisNexis To Buy Seisint For $775 Million: Data Firm's Matrix Tool Generated Controversy," *Washington Post,* July 15, 2004; online at http://www.washingtonpost.com/wp-dyn/articles/A50577-2004Jul14.html.

[100] John Markoff, "Experts Say Technology Is Widely Disseminated Inside and Outside Military," *New York Times*, May 21, 2003; online at http://www.nytimes.com/2003/05/21/international/worldspecial/21PROG.html.

[101] Michael J. Sniffen, "Controversial Terror Research Lives On," Associated Press, February 23, 2004; available online at http://www.washingtonpost.com/wp-dyn/articles/A63582-2004Feb23.html. Bill Powell, "Inside the CIA," *Fortune*, Sept. 29, 2003.

[102] General Accounting Office, "Data Mining: Federal Efforts Cover a Wide Range of Uses," GAO-04-548, May 2004; online at http://www.gao.gov/new.items/d04548.pdf. The CIA and NSA did not participate in the GAO's survey.

[103] See Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law & Commercial Regulation,* Vol. 29 No. 4 (Summer 2004).

[104] Chris Hoofnagle, "Barriers to the Constitutional Right to Privacy: Big Business is keeping an eye on you," *San Francisco Chronicle,* January 29, 2004; online at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/01/29/EDGH14JBAN1.DTL.

[105] "Experian partners with Best Buy: INSOURCE data contributes to Best Buy's successful Customer Relationship Management (CRM) strategy," Experian brochure, online at http://www.experian.com/case_studies/best_buy.pdf.

[106] Abacus Direct slide show, untitled, online at http://www.abacus-direct.com/resource/planningtools/Acquisition.ppt. Or see Experian, "Harnessing the power of consumer data," white paper, p. 7; online at http://www.experian.com/whitepapers/experian%5fdata%5fwhite%5fpaper%5f2002.pdf.

[107] See information on EPIC Freedom of Information Act lawsuit; online at http://www.epic.org/privacy/choicepoint/default.html; Glenn R. Simpson, "Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint" Wall Street Journal, April 13, 2001; William Matthews, "Commercial database use flagged," Federal Computer Week, January 16, 2002; online at http://www.fcw.com/fcw/articles/2002/0114/web-epic-01-16-02.asp.

[108] Seisint Inc., "Seisint's FACTS ™ For The Matrix Project," September 29, 2003, p. 27; online at http://www.aclu.org/Privacy/Privacy.cfm?ID=15233&c=130. Institute for Intergovernmental Research, "Application for Federal Assistance to the Office of Justice Programs Bureau of Justice Assistance," September 24, 2002, in possession of ACLU.

[109] Hoofnagle "Little Helpers," 611.

[110] LexisNexis, "Exhibit B: Lexis-Nexis Select Limited Distribution Authorized Use List" (document obtained by EPIC from the U.S. Marshalls Service); online at http://epic.org/privacy/choicepoint/cpusms7.30.02e.pdf. Cited in Hoofnagle, "Little Helpers," 604.

[111] Hoofnagle "Little Helpers," 607-610.

[112] Martin Finucane, "Cop on the beat now a walking database," Associated Press, June 24, 2004; available online at http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20040624/APN/406240822.

[113] Christian Parenti, *The Soft Cage* (New York: Basic Books, 2003), 92-95; Donner, 414-451.

[114] These points are made in a different context in Jane Mayer, "Contract Sport: What did the Vice-President do for Halliburton?" *The New Yorker*, Feb. 16, 2004; online at http://www.newyorker.com/fact/content/?040216fa_fact.

[115] Patrick Howe, "Growing use of private police network raises concerns," Associated Press, October 30, 20032003; available online at http://www.interesting-people.org/archives/interesting-people/200310/msg00220.html. Patrick Howe, "Expert questions database's legality," Associated Press, December 2, 2003; available online at http://www.twincities.com/mld/pioneerpress/news/local/7391055.htm. Patrick Howe, "Minnesota Public Safety: Police Want Database back," Associated Press, February 16, 2004; available online at http://www.sanluisobispo.com/mld/twincities/news/7962881.htm.

[116] Robert O'Harrow Jr. and Liz Leyden, "U.S. Helped Fund License Photo Database," *Washington Post*, February 18, 1999;

online at http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=business/specials/privacy/robertoharrow&contentId=A48643-1999Feb18. Declan McCullagh, "Smile for the U.S. Secret Service," *Wired News*, September 7, 1999.

[117] Jeffrey Rosen, "Silicon Valley's Spy Game," *New York Times Magazine*, April 14, 2002

[118] "Xybernaut – Wearable Computing – Face Recognition for Public Safety," Email from Xybernaut Corp. executive to official at Dallas Fort-Worth Airport, September 18, 2001, in possession of ACLU.

[119] Bob Davis, "Massive Federal R&D Initiative To Fight Terror Is Under Way," *Wall Street Journal*, November 25, 2002. Paul Magnusson and Mike McNamee, "Welcome to Security Nation," *BusinessWeek*, June 14, 2004; online at http://www.businessweek.com/magazine/content/04_24/b3887036_mz011.htm. See also Brendan I. Koerner, "The Security Traders," *Mother Jones*, September 1, 2002; available online at http://www.newamerica.net/index.cfm?pg=article&pubID=1023.

[120] Megan Lisagor, "TSA awards passenger screening contract," *Federal Computer Week*, March 4, 2004; online at http://www.fcw.com/fcw/articles/2003/0310/news-tsa-03-10-03.asp.

[121] Center for Public Integrity, "The Buying of the President 2004: General Wesley K. Clark," undated. Online at http://www.bop2004.org/bop2004/candidate.aspx?cid=12&act=bio.

[122] United States Senate, Office of Public Records, Lobby Filing Disclosures; online at http://sopr.senate.gov/.

[123] Philip Shenon, "Former Domestic Security Aides Switch to Lobbying," *New York Times*, April 29, 2003; online at http://www.nytimes.com/2003/04/29/politics/29HOME.html.

[124] Adam Mayle and Alex Knott, "Outsourcing Big Brother: Office of Total Information Awareness Relies on Private Sector to Track Americans," Center for Public Integrity, December 17, 20022002; online at http://www.public-i.org/dtaweb/report.asp?ReportID=484. William New, "Back to the Future," *National Journal*, June 14, 2002.

[125] Robert O'Harrow Jr., "U.S. Backs Florida's New Counterterrorism Database," *Washington Post*, August 6, 2003; online at http://www.washingtonpost.com/ac2/wp-dyn/A21872-2003Aug5.

[126] Paul Rogers and Elise Ackerman, "Oracle boss urges national ID cards, offers free software," *Mercury News*, September 22, 2001.

[127] See for example, Robert O'Harrow Jr., "Facial Recognition System Considered For U.S. Airports," *Washington Post*, September 24, 2001; online at http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A14273-2001Sep23.

[128] House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, "Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001," December 2002, pp. 6-32; online at http://www.gpoaccess.gov/serialset/creports/911.html. National Commission on Terrorist Attacks Upon the United States, Staff Statements #9-12; online at http://www.9-11commission.gov/staff_statements.htm.

[129] The Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[130] In 1967 the Supreme Court finally recognized the right to privacy in telephone conversations in the case *Katz v. U.S.* (389 US 347), reversing the 1928 opinion *Olmstead v. U.S.* (277 US 438).

[131] President Dwight D. Eisenhower, "Farewell Address," January 17, 1961; online at http://eisenhower.archives.gov/farewell.htm.

OTHER SAFE AND FREE REPORTS

Conduct Unbecoming: Pitfalls In The President's Military Commissions (March 2004)

Sanctioned Bias: Racial Profiling Since 9/11 (February 2004)

America's Disappeared: Seeking International Justice For Immigrants Detained After September 11 (January 2004)

A New Era of Discrimination? Why African Americans Should Be Alarmed About the Ashcroft Terrorism Laws (September 2003)

Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You (July 2003)

Seeking Truth From Justice: PATRIOT Propaganda—The Justice Department's Campaign to Mislead The Public About the USA PATRIOT Act (July 2003)

Independence Day 2003: Main Street America Fights the Federal Government's Insatiable Appetite for New Powers in the Post 9/11 Era (July 2003)

Freedom Under Fire: Dissent in Post-9/11 America (May 2003)

Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society (January 2003)

Insatiable Appetite: The Government's Demand for Unnecessary Powers After September 11 (October 2002)

Civil Liberties After 9/11: The ACLU Defends Freedom (September 2002)

National Headquarters
125 Broad Street, 18th Fl.
New York, NY 10004-2400
(212) 549-2500
www.aclu.org