Bigger Monster, Weaker Chains:

The Growth of an American Surveillance Society

By Jay Stanley and Barry Steinhardt

December 2002

ACLU
AMERICAN CIVIL LIBERTIES UNION
Technology and Liberty Program

The American Civil Liberties Union is the nation's premier guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and freedoms guaranteed by the Constitution and laws of the United States.

American Civil Liberties Union

National Headquarters

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

Officers and Directors

Bigger Monster, Weaker Chains:

The Growth of an American Surveillance Society

By Jay Stanley and Barry Steinhardt

December 2002

ACLU
AMERICAN CIVIL LIBERTIES UNION
Technology and Liberty Program

Preface

There is no shortage of stories in the media today about the continuing assault on our privacy. But while the latest surveillance program or privacy-invading gadget always receives ample coverage, it is much rarer to find stories that connect the dots and describe the overall impact on privacy in the United States. And without that big picture, the importance of the individual pieces often gets lost.

This new report from the American Civil Liberties Union seeks to provide greater understanding of how our activities are increasingly being tracked and recorded, and how all that data could be drawn together from different sources to create a single high-resolution image of our private lives.

For decades, the notion of a "surveillance society," where every facet of our private lives is monitored and recorded, has sounded abstract, paranoid or far-fetched to many people.

No more! The public's recent introduction to the Pentagon's "Total Information Awareness" project, which seeks to tie together every facet of our private lives in one big surveillance scheme, has provided a stunning lesson in the realities of the new world in which we live. The revelations about the Total Information Awareness program have given the public a sudden introduction to the concept of "data surveillance," and an early glimmer of the technological potential for a surveillance society. It has also confirmed the national security and law enforcement establishments' hunger for such surveillance.

Yet too many people still do not understand the danger, do not grasp just how radical an increase in surveillance by both the government and the private sector is becoming possible, or do not see that the danger stems not just from a single government program, but from a number of parallel developments in the worlds of technology, law, and politics. In this report, the ACLU seeks to flesh out these trends, and, by setting down various developments together in one place, to illuminate the overall danger and what can be done to eliminate it.

The surveillance monster is getting bigger and stronger by the day. But the American Civil Liberties Union believes that it is not too late to build a system of law that can chain it. It is not too late to take back our data.

Introduction

Privacy and liberty in the United States are at risk. A combination of lightning-fast technological innovation and the erosion of privacy protections threatens to transform Big Brother from an oft-cited but remote threat into a very real part of American life. We are at risk of turning into a Surveillance Society.

The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech way to invade people's privacy, from face recognition to implantable microchips, data-mining, DNA chips, and even "brain wave fingerprinting." The fact is, there are no longer any *technical* barriers to the Big Brother regime portrayed by George Orwell.

Even as this surveillance monster grows in power, we are weakening the legal chains that keep it from trampling our lives. We should be responding to intrusive new technologies by building stronger restraints to protect our privacy; instead, we are doing the opposite – loosening regulations on government surveillance, watching passively as private surveillance grows unchecked, and contemplating the introduction of tremendously powerful new surveillance infrastructures that will tie all this information together.

A gradual weakening of our privacy rights has been underway for decades, but many of the most startling developments have come in response to the terrorist attacks of September 11. But few of these hastily enacted measures are likely to increase our protection against terrorism. More often than not, September 11 has been used as a pretext to loosen constraints that law enforcement has been chafing under for years.

It doesn't require some apocalyptic vision of American democracy being replaced by dictatorship to worry about a surveillance society. There is a lot of room for the United States to become a meaner, less open and less just place without any radical change in government. All that's required is the continued construction of new surveillance technologies and the simultaneous erosion of privacy protections.

It's not hard to imagine how in the near future we might see scenarios like the following:

- An African-American man from the central city visits an affluent white suburb to attend a co-worker's barbeque. Later that night, a crime takes place elsewhere in the neighborhood. The police review surveillance camera images, use face recognition to identify the man, and pay him a visit at home the next day. His trip to the suburbs where he "didn't belong" has earned him an interrogation from suspicious police.

- A tourist walking through an unfamiliar city happens upon a sex shop. She stops to gaze at several curious items in the store's window before moving along. Unbeknownst to her, the store has set up the newly available "Customer Identification System," which detects a signal being emitted by a computer chip in her driver's license and records her identity and the date, time, and duration of her brief look inside the window. A week later, she gets a solicitation in the mail mentioning her "visit" and embarrassing her in front of her family.

Such possibilities are only the tip of the iceberg. The media faithfully reports the latest surveillance gadgets and the latest moves to soften the rules on government spying, but rarely provides the big picture. That is unfortunate, because each new threat to our privacy is much more significant as part of the overall trend than it seems when viewed in isolation. When these monitoring technologies and techniques are combined, they can create a surveillance network far more powerful than any single one would create on its own.

The good news is that these trends can be stopped. As the American people realize that each new development is part of this larger story, they will give more and more weight to protecting privacy, and support the measures we need to preserve our freedom.

The Growing Surveillance Monster

In the film *Minority Report,* which takes place in the United States in the year 2050, people called "Pre-cogs" can supposedly predict future crimes, and the nation has become a perfect surveillance society. The frightening thing is that except for the psychic Pre-cogs, the technologies of surveillance portrayed in the film already exist or are in the pipeline. Replace the Pre-cogs with "brain fingerprinting" – the supposed ability to ferret out dangerous tendencies by reading brain waves – and the film's entire vision no longer lies far in the future. Other new privacy invasions are coming at us from all directions, from video and data surveillance to DNA scanning to new data-gathering gadgets.

Video Surveillance

Surveillance video cameras are rapidly spreading throughout the public arena. A survey of surveillance cameras in Manhattan, for example, found that it is impossible to walk around the city without being recorded nearly every step of the way. And since September 11 the pace has quickened, with new cameras being placed not only in some of our most sacred public spaces, such as the National Mall in Washington and the Statue of Liberty in New York harbor, but on ordinary public streets all over America.

Video surveillance may be on the verge of a revolutionary expansion in American Life.

As common as video cameras have become, there are strong signs that, without public action, video surveillance may be on the verge of a revolutionary expansion in American life. There are three factors propelling this revolution:

1. **Improved technology.** Advances such as the digitization of video mean cheaper cameras, cheaper transmission of far-flung video feeds, and cheaper storage and retrieval of images.

2. **Centralized surveillance.** A new centralized surveillance center in Washington, DC is an early indicator of what technology may bring. It allows officers to view images from video cameras across the city – public buildings and streets, neighborhoods, Metro stations, and even schools. With the flip of a switch, officers can zoom in on people from cameras a half-mile away.[1]

3.Unexamined assumptions that cameras provide security. In the wake of the September 11 attacks, many embraced surveillance as the way to prevent future attacks and prevent crime. But it is far from clear how cameras will increase security. U.S. government experts on security technology, noting that "monitoring video screens is both boring and mesmerizing," have found in experiments that after only 20 minutes of watching video monitors, "the attention of most individuals has degenerated to well below acceptable levels."[2] In addition, studies of cameras' effect on crime in Britain, where they have been extensively deployed, have found no conclusive evidence that they have reduced crime.[3]

These developments are creating powerful momentum toward pervasive video surveillance of our public spaces. If centralized video facilities are permitted in Washington and around the nation, it is inevitable that they will be expanded – not only in the number of cameras but also in their power and ability. It is easy to foresee inexpensive, one-dollar cameras being distributed throughout our cities and tied via wireless technology into a centralized police facility where the life of the city can be monitored. Those video signals could be stored indefinitely in digital form in giant but inexpensive databases, and called up with the click of a mouse at any time. With face recognition, the video records could even be indexed and searched based on who the systems identify – correctly, or all to often, incorrectly.

Several airports around the nation, a handful of cities, and even the National Park Service at the Statue of Liberty have installed face recognition. While not nearly reliable enough to be effective as a security application[4], such a system could still violate the privacy of a significant percentage of the citizens who appeared before it (as well as the privacy of those who do not appear before it but are falsely identified as having done so). Unlike, say, an iris scan, face recognition doesn't require the knowledge, consent, or participation of the subject; modern cameras can easily view faces from over 100 yards away.

Further possibilities for the expansion of video surveillance lie with unmanned aircraft, or drones, which have been used by the military and the CIA overseas for reconnaissance, surveillance, and targeting. Controlled from the ground, they can stay airborne for days at a time. Now there is talk of deploying them domestically. Senate Armed Services Committee Chairman John Warner (R, VA) said in December 2002 that he wants to explore their use in Homeland Security, and a number of domestic government agencies have expressed interest in deploying them. Drones are likely to be just one of many ways in which improving robotics technology will be applied to surveillance.[5]

The bottom line is that surveillance systems, once installed, rarely remain confined to their original purpose. Once the nation decides to go down the path of seeking security through video surveillance, the imperative to make it work will become overwhelming, and the monitoring of citizens in public places will quickly become pervasive.

It will soon be possible to recreate an individual's activities with such detail that it becomes no different from being followed around with a video camera.

Data Surveillance

An insidious new type of surveillance is becoming possible that is just as intrusive as video surveillance – what we might call "data surveillance." Data surveillance is *the collection of information about an identifiable individual, often from multiple sources, that can be assembled into a portrait of that person's activities.*[6] Most com-

puters are programmed to automatically store and track usage data, and the spread of computer chips in our daily lives means that more and more of our activities leave behind "data trails." It will soon be possible to combine information from different sources to recreate an individual's activities with such detail that it becomes no different from being followed around all day by a detective with a video camera.

Some think comprehensive public tracking will make no difference, since life in public places is not "private" in the same way as life inside the home. This is wrong; such tracking would represent a radical change in American life. A woman who leaves her house, drives to a store, meets a friend for coffee, visits a museum, and then returns home may be in public all day, but her life is still private in that she is the only one who has an overall view of how she spent her day. In America, she does not expect that her activities are being watched or tracked in any systematic way – she expects to be left alone. But if current trends continue, it will be impossible to have any contact with the outside world that is not watched and recorded.

The Commodification of Information

A major factor driving the trend toward data surveillance forward is the commodification of personal information by corporations. As computer technology exploded in recent decades, making it much easier to collect information about what Americans buy and do, companies came to realize that such data is often very valuable. The expense of marketing efforts gives businesses a strong incentive to know as much about consumers as possible so they can focus on the most likely new customers. Surveys, sweepstakes questionnaires, loyalty programs and detailed product registration forms have proliferated in American life – all aimed at gathering information about consumers. Today, any consumer activity that is *not* being tracked and recorded is increasingly being viewed by businesses as money left on the table.

On the Internet, where every mouse click can be recorded, the tracking and profiling of consumers is even more prevalent. Web sites can not only track what consumers buy, but what they *look at* – and for how long, and in what order. With the end of the Dot Com era, personal information has become an even more precious source of hard cash for those Internet ventures that survive. And of course Americans use the Internet not just as a shopping mall, but to research topics of interest, debate political issues, seek support for personal problems, and many other purposes that can generate deeply private information about their thoughts, interests, lifestyles, habits, and activities.

Unlike other medical information, DNA is a unique combination: both difficult to keep confidential and extremely revealing about us.

Genetic Privacy

The relentless commercialization of information has also led to the breakdown of some longstanding traditions, such as doctor-patient confidentiality. Citizens share some of their most intimate and embarrassing secrets with their doctors on the old-fashioned assumption that their conversations are confidential. Yet those details are routinely shared with insurance companies, researchers, marketers, and employers. An insurance trade organization called the Medical Information Bureau even keeps a centralized medical database with records on millions of patients. Weak new medical privacy rules will do little to stop this behavior.

An even greater threat to medical privacy is looming: genetic information. The increase in DNA analysis for medical testing, research, and other purposes will accelerate sharply in coming years, and will increasingly be incorporated into routine health care.

Unlike other medical information, genetic data is a unique combination: both difficult to keep confidential and extremely revealing about us. DNA is very easy to acquire because we constantly slough off hair, saliva, skin cells and other samples of our DNA (household dust, for example, is made up primarily of dead human skin cells). That means that no matter how hard we strive to keep our genetic code private, we are always vulnerable to other parties' secretly testing samples of our DNA. The issue will be intensified by the development of cheap and efficient DNA chips capable of reading parts of our genetic sequences.

Gramm-Leach effectively gives financial institutions permission to sell their customers' financial data to anyone they choose.

Already, it is possible to send away a DNA sample for analysis. A testing company called Genelex reports that it has amassed 50,000 DNA samples, many gathered surreptitiously for paternity testing. "You'd be amazed," the company's CEO told U.S. News & World Report. "Siblings have sent in mom's discarded Kleenex and wax from her hearing aid to resolve the family rumors."[7]

Not only is DNA easier to acquire than other medical information, revealing it can also have more profound consequences. Genetic markers are rapidly being identified for all sorts of genetic diseases, risk factors, and other characteristics. None of us knows what time bombs are lurking in our genomes.

The consequences of increased genetic transparency will likely include:

- **Discrimination by insurers.** Health and life insurance companies could collect DNA for use in deciding who to insure and what to charge them, with the result that a certain proportion of the population could become uninsurable. The insurance industry has already vigorously opposed efforts in Congress to pass meaningful genetic privacy and discrimination bills.

- **Employment discrimination.** Genetic workplace testing is already on the rise, and the courts have heard many cases. Employees desiring healthy, capable workers will always have an incentive to discriminate based on DNA – an incentive that will be even stronger as long as health insurance is provided through the workplace.

- **Genetic spying.** Cheap technology could allow everyone from schoolchildren to dating couples to nosy neighbors to routinely check out each other's genetic codes. A likely high-profile example: online posting of the genetic profiles of celebrities or politicians.

Financial privacy

Like doctor-patient confidentiality, the tradition of privacy and discretion by financial institutions has also collapsed; financial companies today routinely put the details of their customers' financial lives up for sale.

A big part of the problem is the Gramm-Leach-Bliley Act passed by Congress in 1999. Although Gramm-Leach is sometimes described as a "financial privacy law," it created a very weak privacy standard – so weak, in fact, that far from protecting Americans' financial privacy, the law has had the effect of ratifying the increasing abandonment of customer privacy by financial companies.

Gramm-Leach effectively gives financial institutions permission to sell their customers' financial data to anyone they choose. That includes the date, amount, and recipient of credit card charges or checks a customer has written; account balances; and information about the flow of deposits and withdrawals through an account. Consumers provide a tremendous amount of information about themselves when they fill out applications to get a loan, buy insurance, or purchase securities, and companies can also share that information. In fact, the only information a financial company may NOT give out about you is your account number.

Under Gramm-Leach, you get no privacy unless you file complex paperwork, following a financial institution's precise instructions before a deadline they set, and repeating the process for each and every financial service provider who may have data about you. And it is a process that many companies intentionally make difficult and cumbersome; few let consumers "opt out" of data sharing through a Web site or phone number, or even provide a self-addressed envelope.

Gramm-Leach is an excellent example of the ways that privacy protections are being weakened even as the potential for privacy invasion grows.

New Data-Gathering Technologies

The discovery by businesses of the monetary value of personal information and the vast new project of tracking the habits of consumers has been made possible by advances in computers, databases and the Internet. In the near future, other new technologies will continue to fill out the mosaic of information it is possible to collect on every individual. Examples include:

- **Cell phone location data**. The government has mandated that manufacturers make cell phones capable of automatically reporting their location when an owner dials 911. Of course, those phones are capable of tracking their location at other times as well. And in applying the rules that protect the privacy of telephone records to this location data, the government is weakening those rules in a way that allows phone companies to collect and share data about the location and movements of their customers.

- **Biometrics**. Technologies that identify us by unique bodily attributes such as our fingerprints, faces, iris patterns, or DNA are already being proposed for inclusion on national ID cards and to identify airline passengers. Face recognition is spreading. Fingerprint scanners have been introduced as security or payment mechanisms in office buildings, college campuses, grocery stores and even fast-food restaurants. And several companies are working on DNA chips that will be able to instantly identify individuals by the DNA we leave behind everywhere we go.

- **Black boxes**. All cars built today contain computers, and some of those computers are being programmed in ways that are not necessarily in the interest of owners. An increasing number of cars contain devices akin to the "black boxes" on aircraft that record details about a vehicle's operation and movement. Those devices can "tattle" on car owners to the police or insurance

investigators. Already, one car rental agency tried to charge a customer for speeding after a GPS device in the car reported the transgression back to the company. And cars are just one example of how products and possessions can be programmed to spy and inform on their owners.

RFID chips will allow everyday objects to "talk" to each other – or anyone else who is listening.

- **RFID chips**. RFID chips, which are already used in such applications as toll-booth speed passes, emit a short-range radio signal containing a unique code that identifies each chip. Once the cost of these chips falls to a few pennies each, plans are underway to affix them to products in stores, down to every can of soup and tube of toothpaste. They will allow everyday objects to "talk" to each other – or to anyone else who is listening. For example, they could let market researchers scan the contents of your purse or car from five feet away, or let police officers scan your identification when they pass you on the street.

- **Implantable GPS chips**. Computer chips that can record and broadcast their location have also been developed. In addition to practical uses such as building them into shipping containers, they can also serve as location "bugs" when, for example, hidden by a suspicious husband in a wife's purse. And they can be implanted under the skin (as can RFID chips).

If we do not act to reverse the current trend, data surveillance – like video surveillance – will allow corporations or the government to constantly monitor what individual Americans do every day. Data surveillance would cover *everyone*, with records of every transaction and activity squirreled away until they are sucked up by powerful search engines, whether as part of routine security checks, a general sweep for suspects in an unsolved crime, or a program of harassment against some future Martin Luther King.

Government Surveillance

Data surveillance is made possible by the growing ocean of privately collected personal data. But who would conduct that surveillance? There are certainly business incentives for doing so; companies called data aggregators (such as Acxiom and ChoicePoint) are in the business of compiling detailed databases on individuals and then selling that information to others. Although these companies are invisible to the average person, data aggregation is an enormous, multi-billion-dollar industry. Some databases are even "co-ops" where participants agree to contribute data about their customers in return for the ability to pull out cross-merchant profiles of customers' activities.

The biggest threat to privacy, however, comes from the government. Many Americans are naturally concerned about corporate surveillance, but only the government has the power to take away liberty – as has been demonstrated starkly by the post-September 11 detention of suspects without trial as "enemy combatants."

In addition, the government has unmatched power to centralize all the private sector data that is being generated. In fact, the distinction between government and private-sector privacy invasions is fading

quickly. The Justice Department, for example, reportedly has an $8 million contract with data aggregator ChoicePoint that allows government agents to tap into the company's vast database of personal information on individuals.[8] Although the Privacy Act of 1974 banned the government from maintaining information on citizens who are not the targets of investigations, the FBI can now evade that requirement by simply purchasing information that has been collected by the private sector. Other proposals – such as the Pentagon's "Total Information Awareness" project and airline passenger profiling programs – would institutionalize government access to consumer data in even more far-reaching ways (see below).

Government Databases

The government's access to personal information begins with the thousands of databases it maintains on the lives of Americans and others. For instance:

- The FBI maintains a giant database that contains millions of records covering everything from criminal records to stolen boats and databases with millions of computerized fingerprints and DNA records.

- The Treasury Department runs a database that collects financial information reported to the government by thousands of banks and other financial institutions.

- A "new hires" database maintained by the Department of Health and Human Services, which contains the name, address, social security number, and quarterly wages of every working person in the U.S.

- The federal Department of Education maintains an enormous information bank holding years worth of educational records on individuals stretching from their primary school years through higher education. After September 11, Congress gave the FBI permission to access the database without probable cause.

- State departments of motor vehicles of course possess millions of up-to-date files containing a variety of personal data, including photographs of most adults living in the United States.

The distinction between government and private-sector privacy invasions is fading quickly.

Communications Surveillance

The government also performs an increasing amount of eavesdropping on electronic communications. While technologies like telephone wiretapping have been around for decades, today's technologies cast a far broader net. The FBI's controversial "Carnivore" program, for example, is supposed to be used to tap into the e-mail traffic of a particular individual. Unlike a telephone wiretap, however, it doesn't cover just one device but (because of how the Internet is built) filters through *all* the traffic on the Internet Service Provider to which it has been attached. The only thing keeping the government from trolling through all this traffic is software instructions that are written by the government itself. (Despite that clear conflict of interest, the FBI has refused to allow independent inspection and oversight of the device's operation.)

Another example is the international eavesdropping program codenamed Echelon. Operated by a part-

nership consisting of the United States, Britain, Canada, Australia, and New Zealand, Echelon reportedly grabs e-mail, phone calls, and other electronic communications from its far-flung listening posts across most of the earth. (U.S. eavesdroppers are not supposed to listen in on the conversations of Americans, but the question about Echelon has always been whether the intelligence agencies of participating nations can set up reciprocal, back-scratching arrangements to spy on each others' citizens.) Like Carnivore, Echelon may be used against particular targets, but to do so its operators must sort through massive amounts of information about potentially millions of people. That is worlds away from the popular conception of the old wiretap where an FBI agent listens to one line. Not only the volume of intercepts but the potential for abuse is now exponentially higher.

The "Patriot" Act

The potential for the abuse of surveillance powers has also risen sharply due to a dramatic post-9/11 erosion of legal protections against government surveillance of citizens. Just six weeks after the September 11 attacks, a panicked Congress passed the "USA PATRIOT Act," an overnight revision of the nation's surveillance laws that vastly expanded the government's authority to spy on its own citizens and reduced checks and balances on those powers, such as judicial oversight. The government never demonstrated that restraints on surveillance had contributed to the attack, and indeed much of the new legislation had nothing to do with fighting terrorism. Rather, the bill represented a successful use of the terrorist attacks by the FBI to roll back unwanted checks on its power. The most powerful provisions of the law allow for:

- **Easy access to records**. Under the PATRIOT Act, the FBI can force anyone to turn over records on their customers or clients, giving the government unchecked power to rifle through individuals' financial records, medical histories, Internet usage, travel patterns, or any other records. Some of the most invasive and disturbing uses permitted by the Act involve government access to citizens' reading habits from libraries and bookstores. The FBI does not have to show suspicion of a crime, can gag the recipient of a search order from disclosing the search to anyone, and is subject to no meaningful judicial oversight.

- **Expansion of the "pen register" exception in wiretap law**. The PATRIOT Act expands exceptions to the normal requirement for probable cause in wiretap law.[9] As with its new power to search records, the FBI need not show probable cause or even reasonable suspicion of criminal activity, and judicial oversight is essentially nil.

- **Expansion of the intelligence exception in wiretap law**. The PATRIOT Act also loosens the evidence needed by the government to justify an intelligence wiretap or physical search. Previously the law allowed exceptions to the Fourth Amendment for these kinds of searches only if "the purpose" of the search was to gather foreign intelligence. But the Act changes "the purpose" to "a significant purpose," which lets the government circumvent the Constitution's probable cause requirement even when its main goal is ordinary law enforcement.[10]

- **More secret searches**. Except in rare cases, the law has always required that the subject of a search be notified that a search is taking place. Such notice is a crucial check on the government's power because it forces the authorities to operate in the open and allows the subject of searches to challenge their validity in court. But the PATRIOT Act allows the government to conduct searches without notifying the subjects until long after the search has been executed.

Under these changes and other authorities asserted by the Bush Administration, U.S. intelligence agents could conduct a secret search of an American citizen's home, use evidence found there to declare him an "enemy combatant," and imprison him without trial. The courts would have no chance to review these decisions – indeed, they might never even find out about them.[11]

The "TIPS" Program

In the name of fighting terrorism, the Bush Administration has also proposed a program that would encourage citizens to spy on each other. The Administration initially planned to recruit people such as letter carriers and utility technicians, who, the White House said, are "well-positioned to recognize unusual events." In the face of fierce public criticism, the Administration scaled back the program, but continued to enlist workers involved in certain key industries. In November 2002 Congress included a provision in the Homeland Security Act prohibiting the Bush Administration from moving forward with TIPS.

Attorney General John Ashcroft issued new guidelines that significantly increase the freedom of federal agents to conduct surveillance on Americans.

Although Congress killed TIPS, the fact that the Administration would pursue such a program reveals a disturbing disconnect with American values and a disturbing lack of awareness of the history of governmental abuses of power. Dividing citizen from citizen by encouraging mutual suspicion and reporting to the government would dramatically increase the government's power by extending surveillance into every nook and cranny of American society. Such a strategy was central to the Soviet Union and other totalitarian regimes.

Loosened Domestic Spying Regulations

In May 2002, Attorney General John Ashcroft issued new guidelines on domestic spying that significantly increase the freedom of federal agents to conduct surveillance on American individuals and organizations. Under the new guidelines, FBI agents can infiltrate "any event that is open to the public," from public meetings and demonstrations to political conventions to church services to 12-step programs. This was the same basis upon which abuses were carried out by the FBI in the 1950s and 1960s, including surveillance of political groups that disagreed with the government, anonymous letters sent to the spouses of targets to try to ruin their marriages, and the infamous campaign against Martin Luther King, who was investigated and harassed for decades. The new guidelines are purely for spying on Americans; there is a separate set of Foreign Guidelines that cover investigations inside the U.S. of foreign powers and terrorist organizations such as Al Qaeda.

Like the TIPS program, Ashcroft's guidelines sow suspicion among citizens and extend the government's surveillance power into the capillaries of American life. It is not just the reality of government surveillance that chills free expression and the freedom that Americans enjoy. The same negative effects come when we are constantly forced to wonder whether we *might* be under observation – whether the person sitting next to us is secretly informing the government that we are "suspicious."

The Synergies of Surveillance

Multiple surveillance techniques added together are greater than the sum of their parts. One example is face recognition, which combines the power of computerized software analysis, cameras, and databases to seek matches between facial images. But the real synergies of surveillance come into play with data collection.

The growing piles of data being collected on Americans represent an enormous invasion of privacy, but our privacy has actually been protected by the fact that all this information still remains scattered across many different databases. As a result, there exists a pent-up capacity for surveillance in American life today – a capacity that will be fully realized if the government, landlords, employers, or other powerful forces gain the ability to *draw together* all this information. A particular piece of data about you – such as the fact that you entered your office at 10:29 AM on July 5, 2001 – is normally innocuous. But when enough pieces of that kind of data are assembled together, they add up to an extremely detailed and intrusive picture of an individual's life and habits.

Data Profiling and "Total Information Awareness"

Just how real this scenario is has been demonstrated by another ominous surveillance plan to emerge from the effort against terrorism: the Pentagon's "Total Information Awareness" program. The aim of this program is to give officials easy, unified access to every possible government and commercial database in the world.[12] According to program director John Poindexter, the program's goal is to develop "ultra-large-scale" database technologies with the goal of "treating the world-wide, distributed, legacy databases as if they were one centralized database." The program envisions a "full-coverage database containing all information relevant to identifying" potential terrorists and their supporters. As we have seen, the amount of available information is mushrooming by the day, and will soon be rich enough to reveal much of our lives.

Programs like TIA involve turning the defense capabilities of the United States inward and applying them to American people.

The TIA program, which is run by the Defense Advanced Research Projects Agency (DARPA), not only seeks to bring together the oceans of data that are already being collected on people, but would be designed to afford what DARPA calls "easy future scaling" to embrace new sources of data as they become available. It would also incorporate other work being done by the military, such as their "Human Identification at a Distance" program, which seeks to allow identification and tracking of people from a distance, and therefore without their permission or knowledge.[13]

Although it has not received nearly as much media attention, a close cousin of TIA is also being created in the context of airline security. This plan involves the creation of a system for conducting background checks on individuals who wish to fly and then separating out either those who appear to be the most trustworthy passengers (proposals known as "trusted traveler") or flagging the least trustworthy (a proposal known as CAPS II, for Computer Assisted Passenger Screening) for special attention.

The *Washington Post* has reported that work is being done on CAPS II with the goal of creating a "vast air security screening system designed to instantly pull together every passenger's travel history and liv-

ing arrangements, plus a wealth of other personal and demographic information" in the hopes that the authorities will be able to "profile passenger activity and intuit obscure clues about potential threats." The government program would reportedly draw on enormous stores of personal information from data aggregators and other sources, including travel records, real estate histories, personal associations, credit card records, and telephone records. Plans call for using complex computer algorithms, including highly experimental technologies such as "neural networks," to sort through the reams of new personal information and identify "suspicious" people.[14]

The dubious premise of programs like TIA and CAPS II – that "terrorist patterns" can be ferreted out from the enormous mass of American lives, many of which will inevitably be quirky, eccentric, or riddled with suspicious coincidences – probably dooms them to failure. But failure is not likely to lead these programs to be shut down – instead, the government will begin feeding its computers more and more personal information in a vain effort to make the concept work. We will then have the worst of both worlds: poor security and a super-charged surveillance tool that would destroy Americans' privacy and threaten our freedom.

It is easy to imagine these systems being expanded in the future to share their risk assessments with other security systems. For example, CAPS could be linked to a photographic database and surveillance cameras equipped with face recognition software. Such a system might sound an alarm when a subject who has been designated as "suspicious" appears in public. The Suspicious Citizen could then be watched from a centralized video monitoring facility as he moves around the city.

In short, the government is working furiously to bring disparate sources of information about us together into one view, just as privacy advocates have been warning about for years. That would represent a radical branching off from the centuries-old Anglo-American tradition that the police conduct surveillance only where there is evidence of involvement in wrongdoing. It would seek to protect us by monitoring *everyone* for signs of wrongdoing – in short, by instituting a giant dragnet capable of sifting through the personal lives of Americans in search of "suspicious" patterns. The potential for abuse of such a system is staggering.

The massive defense research capabilities of the United States have always involved the search for ways of outwardly defending our nation. Programs like TIA[15] involve turning those capabilities inward and applying them to the American people – something that should be done, if at all, only with extreme caution and plenty of public input, political debate, checks and balances, and Congressional oversight. So far, none of those things have been present with TIA or CAPS II.

National ID Cards

If Americans allow it, another convergence of surveillance technologies will probably center around a national ID card. A national ID would immediately combine new technologies such as biometrics and RFID chips along with an enormously powerful database (possibly distributed among the 50 states). Before long, it would become an overarching means of facilitating surveillance by allowing far-flung pools of information to be pulled together into a single, incredibly rich dossier or profile of our lives. Before long, office buildings, doctors' offices, gas stations, highway tolls, subways and buses would incorporate the ID card into their security or payment systems for greater efficiency, and data that is currently scattered and disconnected will get organized around the ID and lead to the creation of what amounts to a national database of sensitive information about American citizens.

History has shown that databases created for one purpose are almost inevitably expanded to other uses; Social Security, which was prohibited by federal law from being used as an identifier when it was first created, is a prime example. Over time, a national ID database would inevitably contain a wider and wider range of information and become accessible to more and more people for more and more purposes that are further and further removed from its original justification.

The most likely route to a national ID is through our driver's licenses.

The most likely route to a national ID is through our driver's licenses. Since September 11, the American Association of Motor Vehicle Administrators has been forcefully lobbying Congress for funds to establish nationwide uniformity in the design and content of driver's licenses – and more importantly, for tightly interconnecting the databases that lie behind the physical licenses themselves.

An attempt to retrofit driver's licenses into national ID cards will launch a predictable series of events bringing us toward a surveillance society:

- Proponents will promise that the IDs will be implemented in limited ways that won't devastate privacy and other liberties.

- Once a limited version of the proposals is put in place, its limits as an anti-terrorism measure will quickly become apparent. Like a dam built halfway across a river, the IDs cannot possibly be effective unless their coverage is total.

- The scheme's ineffectiveness – starkly demonstrated, perhaps, by a new terrorist attack – will create an overwhelming imperative to "fix" and "complete" it, which will turn it into the totalitarian tool that proponents promised it would never become.

A perfect example of that dynamic is the requirement that travelers present driver's licenses when boarding airplanes, instituted after the explosion (now believed to have been mechanical in cause) that brought down TWA Flight 800 in 1996. On its own, the requirement was meaningless as a security measure, but after September 11 its existence quickly led to calls to begin tracking and identifying citizens on the theory that "we already have to show ID, we might as well make it mean something."

Once in place, it is easy to imagine how national IDs could be combined with an RFID chip to allow for convenient, at-a-distance verification of ID. The IDs could then be tied to access control points around our public places, so that the unauthorized could be kept out of office buildings, apartments, public transit, and secure public buildings. Citizens with criminal records, poor CAPS ratings or low incomes could be barred from accessing airports, sports arenas, stores, or other facilities. Retailers might add RFID readers to find out exactly who is browsing their aisles, gawking at their window displays from the sidewalk or passing by without looking. A network of automated RFID listening posts on the sidewalks and roads could even reveal the location of all citizens at all times. Pocket ID readers could be used by FBI agents to sweep up the identities of everyone at a political meeting, protest march, or Islamic prayer service.

Conclusion

If we do not take steps to control and regulate surveillance to bring it into conformity with our values, we will find ourselves being tracked, analyzed, profiled, and flagged in our daily lives to a degree we can scarcely imagine today. We will be forced into an impossible struggle to conform to the letter of every rule, law, and guideline, lest we create ammunition for enemies in the government or elsewhere. Our transgressions will become permanent Scarlet Letters that follow us throughout our lives, visible to all and used by the government, landlords, employers, insurance companies and other powerful parties to increase their leverage over average people. Americans will not be able to engage in political protest or go about their daily lives without the constant awareness that we are – or could be – under surveillance. We will be forced to constantly ask of even the smallest action taken in public, "Will this make me look suspicious? Will this hurt my chances for future employment? Will this reduce my ability to get insurance?" The exercise of free speech will be chilled as Americans become conscious that their every word may be reported to the government by FBI infiltrators, suspicious fellow citizens or an Internet Service Provider.

Our transgressions will become permanent Scarlet Letters visible to all and used by the powerful to increase their leverage over average people.

Many well-known commentators like Sun Microsystems CEO Scott McNealy have already pronounced privacy dead. The truth is that a surveillance society does loom over us, and privacy, while not yet dead, is on life support.

Heroic measures are required to save it.

Four main goals need to be attained to prevent this dark potential from being realized: a change in the terms of the debate, passage of comprehensive privacy laws, passage of new laws to regulate the powerful and invasive new technologies that have and will continue to appear, and a revival of the Fourth Amendment to the U.S. Constitution.

1. Changing the Terms of the Debate

In the public debates over every new surveillance technology, the forest too often gets lost for the trees, and we lose sight of the larger trend: the seemingly inexorable movement toward a surveillance society. It will always be important to understand and publicly debate every new technology and every new technique for spying on people. But unless each new development is also understood as just one piece of the larger surveillance mosaic that is rapidly being constructed around us, Americans are not likely to get excited about a given incremental loss of privacy like the tracking of cars through toll booths or the growing practice of tracking consumers' supermarket purchases.

We are being confronted with fundamental choices about what sort of society we want to live in. But unless the terms of the debate are changed to focus on the forest instead of individual trees, too many

Americans will never even recognize the choice we face, and a decision against preserving privacy will be made by default.

2. Comprehensive Privacy Laws

Although broad-based protections against government surveillance, such as the wiretap laws, are being weakened, at least they exist. But surveillance is increasingly being carried out by the private sector – frequently at the behest of government – and the laws protecting Americans against non-governmental privacy invasions are pitifully weak.

In contrast to the rest of the developed world, the U.S. has no strong, comprehensive law protecting privacy – only a patchwork of largely inadequate protections. For example, as a result of many legislators' discomfort over the disclosure of Judge Robert Bork's video rental choices during his Supreme Court confirmation battle, video records are now protected by a strong privacy law. Medical records are governed by a separate, far weaker law that allows for widespread access to extremely personal information. Financial data is governed by yet another "privacy" law – Gramm-Leach – which as we have seen really amounts to a license to share financial information. Another law protects only the privacy of children under age 13 on the Internet. And layered on top of this sectoral approach to privacy by the federal government is a geographical patchwork of constitutional and statutory privacy protections in the states.

We are being confronted with fundamental choices about what sort of society we want to live in.

The patchwork approach to privacy is grossly inadequate. As invasive practices grow, Americans will face constant uncertainty about when and how these complex laws protect them, contributing to a pervasive sense of insecurity. With the glaring exception of the United States, every advanced industrialized nation in the world has enacted overarching privacy laws that protect citizens against private-sector abuses. When it comes to this fundamental human value, the U.S. is an outlaw nation. For example, the European Union bars companies from evading privacy rules by transferring personal information to other nations whose data-protection policies are "inadequate." That is the kind of law that is usually applied to Third World countries, but the EU counts the United States in this category.

We need to develop a baseline of simple and clear privacy protections that crosses all sectors of our lives and give it the force of law. Only then can Americans act with a confident knowledge of when they can and cannot be monitored.

3. New Technologies and New Laws

The technologies of surveillance are developing at the speed of light, but the body of law that protects us is stuck back in the Stone Age. In the past, new technologies that threatened our privacy, such as telephone wiretapping, were assimilated over time into our society. The legal system had time to adapt and reinterpret existing laws, the political system had time to consider and enact new laws or regulations, and the culture had time to absorb the implications of the new technology for daily life. Today, however, change is happening so fast that none of this adaptation has time to take place – a problem

that is being intensified by the scramble to enact unexamined anti-terrorism measures. The result is a significant danger that surveillance practices will become entrenched in American life that would never be accepted if we had more time to digest them.

Since a comprehensive privacy law may never be passed in the U.S. – and certainly not in the near future – law and legal principles must be developed or adapted to rein in particular new technologies such as surveillance cameras, location-tracking devices, and biometrics. Surveillance cameras, for example, must be subject to force-of-law rules covering important details like when they will be used, how long images will be stored, and when and with whom they will be shared.

4. Reviving the Fourth Amendment

> *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.*
>
> – Fourth Amendment to the U.S. Constitution

The Fourth Amendment, the primary Constitutional bulwark against Government invasion of our privacy, was a direct response to the British authorities' use of "general warrants" to conduct broad searches of the rebellious colonists.

Historically, the courts have been slow to adapt the Fourth Amendment to the realities of developing technologies. It took almost 40 years for the U.S. Supreme Court to recognize that the Constitution applies to the wiretapping of telephone conversations.[16]

In recent years – in no small part as the result of the failed "war on drugs" – Fourth Amendment principles have been steadily eroding. The circumstances under which police and other government officials may conduct warrantless searches has been rapidly expanding. The courts have allowed for increased surveillance and searches on the nation's highways and at our "borders" (the legal definition of which actually extends hundreds of miles inland from the actual border). And despite the Constitution's plain language covering "persons" and "effects," the courts have increasingly allowed for warrantless searches when we are outside of our homes and "in public." Here the courts have increasingly found we have no "reasonable expectation" of privacy and that therefore the Fourth Amendment does not apply.

But like other Constitutional provisions, the Fourth Amendment needs to be understood in contemporary terms. New technologies are endowing the government with the 21st Century equivalent of Superman's X-ray vision. Using everything from powerful video technologies that can literally see in the dark, to biometric identification techniques like face recognition, to "brain fingerprinting" that can purportedly read our thoughts, the government is now capable of conducting broad searches of our "persons and effects" while we are going about our daily lives – even while we are in "public."

The Fourth Amendment is in desperate need of a revival. The reasonable expectation of privacy cannot be defined by the power that technology affords the government to spy on us. Since that power is increasingly limitless, the "reasonable expectation" standard will leave our privacy dead indeed.

But all is not yet lost. There is some reason for hope. In an important pre-9/11 case, *Kyllo vs. U.S.*,[17] the Supreme Court held that the reasonable expectation of privacy could not be determined by the power of new technologies. In a remarkable opinion written by conservative Justice Antonin Scalia, the Court held that without a warrant the police could not use a new thermal imaging device that searches for heat sources to conduct what was the functional equivalent of a warrantless search for marijuana cultivation in Danny Kyllo's home.

The Court specifically declined to leave Kyllo "at the mercy of advancing technology." While Kyllo involved a search of a home, it enunciates an important principle: the Fourth Amendment must adapt to new technologies. That principle can and should be expanded to general use. The Framers never expected the Constitution to be read exclusively in terms of the circumstances of 1791.

Notes

1 Jess Bravin, "Washington Police to Play 'I Spy' With Cameras, Raising Concerns," *Wall Street Journal*, Feb. 13, 2002.

2 See http://www.ncjrs.org/school/ch2a_5.html.

3 See http://www.scotcrim.u-net.com/researchc2.htm.

4 The success rate of face recognition technology has been dismal. The many independent findings to that effect include a trial conducted by the U.S. military in 2002, which found that with a reasonably low false-positive rate, the technology had less than a 20% chance of successfully identifying a person in its database who appeared before the camera. See http://www.aclu.org/issues/privacy/FINAL_1_Final_Steve_King.pdf, 17th slide.

5 Richard H.P. Sia, "Pilotless Aircraft Makers Seek Role For Domestic Uses," *CongressDaily*, December 17, 2002.

6 Data surveillance is often loosely referred to as "data mining." Strictly speaking, however, data mining refers to the search for hidden patterns in large, pre-existing collections of data (such as the finding that sales of both beer and diapers rise on Friday nights). Data mining need not involve personally identifiable information. Data surveillance, on the other hand, involves the collection of information about an identifiable individual. Note, however, that when data surveillance is carried out on a mass scale, a search for patterns in people's activities – data mining – can then be conducted as well. This is what appears to be contemplated in the Total Information Awareness and CAPS II programs (see below).

7 Dana Hawkins, "As DNA Banks Quietly Multiply, Who is Guarding the Safe?" *U.S. News & World Report*, Dec. 2, 2002.

8 Glenn R. Simpson, "Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint" *Wall St. Journal*, April 13, 2001.

9 The expanded exception involves what are called "pen register/trap & trace" warrants that collect "addressing information" but not the content of a communication. Those searches are named after devices that were used on telephones to show a list of telephone numbers dialed and received (as opposed to tapping into actual conversations). The PATRIOT Act expands the pen register exception onto the Internet in ways that will probably be used by the government to collect the actual content of communications and that allow nonspecific "nationwide" warrants in violation of the Fourth Amendment's explicit requirement that warrants "must specify the place to be searched."

10 In August, the secret "FISA" court that oversees domestic intelligence spying released an opinion rejecting a Bush Administration attempt to allow criminal prosecutors to use intelligence warrants to evade the Fourth Amendment entirely. The court noted that agents applying for warrants had regularly filed false and misleading information. In November 2002, however, the FISA appeals court (three judges chosen by Supreme Court Chief Justice William Rehnquist), meeting for the first time ever, ruled in favor of the government.

11 See Charles Lane, "In Terror War, 2nd Track for Suspects," *Washington Post,* December 1, 2002. Online at http://www.washingtonpost.com/wp-dyn/articles/A58308-2002Nov30.html.

12 See "Pentagon Plans a Computer System That Would Peek at Personal Data of Americans," *New York Times*, Nov. 9, 2002; "US Hopes to Check Computers Globally," *Washington Post*, Nov. 12, 2002; "The Poindexter Plan," *National Journal*, Sept. 7, 2002.

13 Quotes are from the TIA homepage at http://www.darpa.mil/iao/index.htm and from public 8/2/02 remarks by Poindexter, online at http://www.fas.org/irp/agency/dod/poindexter.html.

14 Robert O'Harrow Jr., "Intricate Screening Of Fliers In Works," *Washington Post*, Feb. 1, 2002, p. A1.

15 The TIA is just one part of a larger post-9/11 expansion of federal research and development efforts. The budget for military R&D spending alone has been increased by 18% in the current fiscal year to a record $58.8 billion. Bob Davis, "Massive Federal R&D Initiative To Fight Terror Is Under Way," *Wall Street Journal*, November 25, 2002.

16 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).

17 190 F.3d 1041, 2001.

Technology and
Liberty Program