

## **Is the US Turning Into a Surveillance Society?**

### **Big Brother is no longer a fiction**

**ACLU Technology and Liberty Program**

**January 2003**

The United States is at risk of turning into a full-fledged surveillance society. A new ACLU report, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society* provides an overview of the many ways in which we are drifting toward a surveillance society, and what we need to do about it.

There are two simultaneous developments behind this trend:

- The tremendous explosion in surveillance-enabling technologies, including databases, computers, cameras, sensors, wireless networks, implantable microchips, GPS, and biometrics. The fact is, Orwell's vision of "Big Brother" is now, for the first time, *technologically* possible.
- Even as this technological surveillance monster grows in our midst, we are weakening the chains that keep it from trampling our privacy (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).

The good news is that the drift toward a surveillance society can be stopped. As the American people realize that each new development is part of this bigger picture, they will give more and more weight to protecting privacy, and support the measures we need to preserve our freedom. Unfortunately, right now the big picture is grim. There are numerous disturbing developments:

### **Video Surveillance**

Surveillance video cameras are rapidly spreading throughout the public arena, with new cameras being placed not only in some of our most sacred public spaces, but on ordinary public streets all over America. And video surveillance may be on the verge of an even greater revolution due to advances in technology like Face Recognition Technology and new attempts to build centralized monitoring facilities.

## 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." As 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.

- **The Commodification of Information**

Today, any consumer activity that is *not* being tracked and recorded is increasingly being viewed by businesses as money left on the table.

- **Internet Privacy**

On the Internet, our activities can be recorded down to the last mouse click.

- **Financial privacy**

The once-firm tradition of privacy and discretion by financial institutions has collapsed, and financial companies today routinely put the details of their customers' financial lives up for sale.

- **New Data-Gathering Technologies**

In the near future, 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, biometrics, computer "black boxes" in cars that "tattle" on their owners, and location-tracking computer chips.

- **Medical & Genetic Privacy**

Medical privacy has collapsed, and genetic information is about to become a central part of health care. Unlike other medical information, genetic data is a unique combination: both difficult to keep confidential and extremely revealing about us.

## Government Surveillance

The biggest threat to privacy comes from the government. Many Americans are naturally concerned about corporate surveillance, but only the government has the power to take away liberty.

- **Government Databases**

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

- **Communications Surveillance**

The government performs an increasing amount of eavesdropping on electronic communications. Examples of the new type of surveillance include the FBI's controversial "Carnivore" program and the international eavesdropping program codenamed Echelon.

- **The "Patriot" Act**

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.

- **Loosened Domestic Spying Regulations**

In May 2002, Attorney General John Ashcroft issued new guidelines that significantly increase the freedom of federal agents to conduct surveillance on American individuals and organizations.

## **The Synergies of Surveillance**

Multiple surveillance techniques added together are greater than the sum of their parts. 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. The real threat to privacy will come when the government, landlords, employers, or other powerful forces gain the ability to *draw together* all this information. Several programs now being discussed or implemented would advance this goal:

- **"Total Information Awareness"**

This Pentagon program aims at giving officials easy, one-stop access to every possible government and commercial database in the world.

- **CAPS II**

A close cousin of TIA is also being created in the context of airline security: Computer Assisted Passenger Screening, or CAPS, which involves collecting a variety of personal information on airline travelers in order to flag those deemed suspicious for special screening.

- **National ID Cards**

Combining new technologies such as biometrics with an enormously powerful database, national ID Cards would become an overarching means of facilitating the tracking and surveillance of Americans.

## **What We Must Do**

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.

Four main goals need to be attained to prevent this dark potential from being realized:

**1. Change the Terms of the Debate**

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 big picture instead of individual privacy stories, too many Americans will never even recognize the choice we face, and a decision against preserving privacy will be made by default.

**2. Enact Comprehensive Privacy Laws**

The US has an inconsistent, patchwork approach to privacy regulation, and 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.

**3. Pass New Laws For New Technologies**

Laws must also be developed 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. Revive the Fourth Amendment**

The Fourth Amendment, the primary Constitutional bulwark against Government invasion of our privacy, is in desperate need of a revival. The Fourth Amendment must be adapted to new technologies; the Framers never expected the Constitution to be read exclusively in terms of the circumstances of 1791.

Copyright © 2003 American Civil Liberties Union  
Reprinted for Fair Use Only.