

# How We Live Now

by JOHN TWELVE HAWKS

We drink our morning coffee with a drop of fear. The television news alternates between staged media events and new threats to our lives: terrorism and airline crashes, global warming and car-jackings, an epidemic of avian flu. All the threats are different, but they have one common theme: it's impossible to truly be safe. Somehow all of us have become victims—or potential victims—of a long list of dangers.

With these threats fresh in our mind, we travel to work tracked by pervasive electronic monitoring systems. There's a Global Positioning device inside our automobile and another within our cell phone; both inform a computer of our exact location. A transponder knows when we approach a toll booth. A transit card records our trip on the subway and stores the information in a central data bank. And everywhere we go, there are surveillance cameras—thousands of them—to photograph and record our image. Some of them are “smart” cameras, linked to computer programs that watch our movements in case we act differently from the rest of the crowd: if we walk too slowly, if we linger outside certain buildings, if we stop to laugh or enjoy the view, our body is highlighted by a red line on a video monitor and a security guard has to decide whether he should call the police.

These two modern conditions—a generalized fear coupled with sophisticated electronic monitoring—shape the world of “The Traveler,” my first novel. Many critics have reviewed the book as science fiction, an idea that amuses me; although “The Traveler” is set toward the end of our decade, all the technical aspects described in the book are either in use at this moment or far along in the development process. I didn't write the book to predict the future; I wanted to use the power of fiction to describe how we live now.

This new technology of control and the wide-scale manipulation of fear combine to create something I call “The Vast Machine.” Does the Machine really exist? Are we living in such an environment? And, if this fiction turns out to be the truth, what difference does it make to our lives? The first icon of the 21st century is the closed-circuit surveillance camera, slowly panning back and forth as we move beneath its gaze. A few years ago, it was estimated that the average person in London was photographed at least 300 times by different CCTV cameras on their way to work; the amount of cameras has probably doubled since the terrorist bombings on the London tube.

Chicago gives us a typical example of the rapid spread of surveillance cameras. There are over 2,000 cameras in the city and hundreds more are introduced every month. Mayor Daley stated that “*The city owns the sidewalks. We own the streets and we own the alleys.*” Then he announced plans to put surveillance cameras in commuter cars, on buses and on the city's street sweeping vehicles.

The outline of a Vast Machine becomes apparent when we examine the new “smart” cameras used in Chicago, London, and Las Vegas. The computers attached to these machines contain a template of what should be determined “normal” behavior for a person. If anyone behaves differently, those actions are immediately detected.

<http://wespeakforfreedom.com>

During the next few years, surveillance cameras will also feed data into computerized facial recognition systems. There are about 80 “nodal points”—unique features—in every person's face. Facial recognition systems transform our unique features into complex algorithms that are checked against a database of driver's licenses and passport photos. The idea that a surveillance camera could identify a stranger in a crowd was thought to be fictional by some of my readers, but first-generation recognition systems have been operational for years. At the January 2000 Super Bowl in Florida, dozens of surveillance cameras automatically scanned every person in the crowd and compared the faces to a database of criminal mug shots.

These days, people are routinely photographed when they pass through airport immigration checkpoints, and that image is compared to the biometric data (fingerprints, iris scan) embedded in the passport. But the new biometric passports to be introduced by the United States reveal another aspect of the Vast Machine. Although the passports are ostensibly being introduced to protect us, they actually make it more dangerous for American tourists in foreign countries.

The passports contain a radio frequency identification chip (RFID) so that all our personal information can be instantly read by a machine at the airport. However, the State Department has refused to encrypt the information embedded in the chip, because it requires more complicated technology that is difficult to coordinate with other countries. This means that our personal information could be read by a machine called a “skimmer” that can be placed in a doorway or a bus stop, perhaps as far as 30 feet away.

The U.S. government isn't concerned by this, but the contents of Paris Hilton's cell phone, which uses the same kind of RFID chip, were skimmed and made public last year. It may not seem like a problem when a semi-celebrity's phone numbers and emails are stolen, but it is quite possible that an American tourist walking down a street in a foreign country will be “skimmed” by a machine that reads the passport in his or her pocket. A terrorist group will be able to decide if the name on the passport indicates a possible target before the tourist reaches the end of the street.

The new RFID passports are a clear indication that protection is not as important to the authorities as the need to acquire easily accessible personal information. The means of acquiring information are expanding every day. Most people realize that the GPS devices in automobiles allow a central computer to determine a car's precise location. But there are also hidden sensors placed in car tires as well as a “black box” under each hood that records car speed and direction (generally used in the event of an accident).

While our location is being tracked, computer programs automatically read and evaluate emails without our knowledge. Carnivore is one of the programs mentioned in my novel. It's a “packet sniffer” developed by the Federal Bureau of Investigation along with a variety of other on-line detection programs—like Packeteer and Coolminer—that reassemble message fragments and analyze data. Like the smart surveillance cameras used in Chicago, the Carnivore programs establish a standard for what is normal, and everything else is automatically judged as being suspicious. Gradually, all these evaluation systems are becoming independent of any direct control.

“The Traveler” describes for the first time in any book the secret computational immunology programs being developed in Britain. These programs behave like the leucocytes floating

[We Speak for Freedom](http://wespeakforfreedom.com)

<http://wespeakforfreedom.com>

through our bloodstream. The programs wander through the Internet, searching, evaluating, and hiding in a person's home PC, until they detect a “dangerous” statement or unusual information. After gathering our personal information, they return to the central computer. There is no reason why they can't easily be programmed to destroy a target computer...such as the one on which you're reading this essay.

Once you look beyond surveillance cameras, you can find the Vast Machine everywhere.

Infrared devices and x-ray machines can “see” through walls of homes and vehicles. New data systems can instantly evaluate ATM and credit card activity, building a computerized image of our personality and buying preferences. Viewed in isolation, each of these technological developments is not a major threat to our privacy. But the growing computational power of computers allows all of these monitoring tools and databases to be combined into one total information system.

In January 2002, former Reagan administration national security advisor John Poindexter was appointed to be the head of the U.S. government's newly formed Information Awareness Office. Poindexter had been convicted in 1990 of five felony counts of lying to Congress, destroying official documents and obstructing congressional inquiries into the Iran-Contra affair, but this didn't seem to disqualify him from his new position.

Under Poindexter's leadership, the IAO proposed a “Total Information Awareness” program that would place all personal information about U.S. citizens in one central database.

According to New York Times columnist William Safire:

*“Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site your visit and email you send and receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into what the Defense Department describes as 'a virtual centralized database.'”*

In his book *“No Place to Hide,”* Washington Post reporter Robert O'Harrow describes how the controversy over Total Information Awareness resulted in public protests and Poindexter's resignation. But TIA did not disappear; it was simply renamed the “Terrorist Information Awareness” program, and the technology was passed on to U.S. intelligence agencies. Poindexter may have lost his job, but his vision lives on.

Total information systems are being developed in every industrial country. In Europe, these systems are almost exclusively controlled by the government. In the United States, weak privacy laws have also given private industry almost unlimited power to create dossiers of every American citizen.

I feel strongly about the growing power of computer monitoring systems, and that belief has a great deal to do with my decision to retain a truly private “private life”—even when dealing with my agent and publisher. It seemed hypocritical for an author to attack the loss of privacy in our society and then display his personal life to promote a book. Although I have avoided the media, however, I've talked to a wide variety of people about these new forms of surveillance. A few people have been disturbed about the intrusion, but many have given a more typical response:

[We Speak for Freedom](http://wespeakforfreedom.com)

<http://wespeakforfreedom.com>

*“They (our leaders) know what's best.”*

*“It's a dangerous world.”*

*“Honest people have nothing to hide.”*

Believing that the government knows what's best is an argument that barely merits a serious discussion. Any high school history student can come up with hundreds of examples of when a king, dictator, or elected official followed a destructive, foolish policy. Democracy doesn't protect our leaders from having a limited, parochial vision. Often a politician's true priority is career self-preservation.

The prompt arrests of the four suspects of the failed July 21 London bombings indicated that surveillance cameras and other elements of our electronic society can help protect our society from terrorists. But in destroying our enemies we run the risk of destroying ourselves—those elements of personal freedom and tolerance that define and sustain our society. We seem to be blindly giving up our rights without asking our elected officials how their actions will truly defeat our enemies.

*“And so what if they know all about me?”* asks the honest citizen. *“I'm good person. I've got nothing to hide.”* This view assumes that the intimate personal information easily found in our computerized system is accurate, secure, and will only be used for your benefit. What if criminals access your information? What if corporations deny you insurance or employment because the wrong data has ended up in your file? What if you simply want to take control over who knows what about you? Obviously, our government needs to know certain facts about us so that elected officials can enforce laws and protect our borders. But during the last few years, information gathering has gone far beyond the standard data shown on a driver's license or income tax form. These days it is easy to target someone and find out his medical condition, the names of his friends, and the titles of the books he's checked out of the library. This data can be used in sophisticated ways to predict behavior.

In every religion, saints and prophets go off alone when they want to talk to God. We need moments of true privacy to evaluate our thoughts and experiences; to decide what we really believe. There is a reason why a curtain—real or symbolic—is placed around the voting booth in a democratic society. If privacy truly disappears, freedom itself will vanish with it.

It's clear that the new computerized technology has resulted in the end of our conventional view of privacy. But a true picture of the way we live now involves more than Carnivore programs and radio frequency chips. The Vast Machine monitors our actions, but it also gives us a reason for that intrusion. The reason is always the same: those in power are working to protect us.

Fear is a necessary part of our survival; the response is programmed into our neurological system. But in the 21st century, modern communications make it possible for everyone to know instantly about any possible danger, however remote, however far in the future. The Internet multiplies these sources of information, relaying threats both real and imagined.

In his insightful book *“The Culture of Fear,”* Barry Glassner shows how many of our specific fears are created and sustained by media manipulation. There can be an enormous discrepancy between what we fear and the reality of what could happen to us. Glassner analyzes several “threats” such as airplane disasters, youth homicide, and road rage, and proves that the chance of any of these dangers harming an individual is virtually nonexistent.

[We Speak for Freedom](http://wespeakforfreedom.com)

<http://wespeakforfreedom.com>

Although Glassner accurately describes the falseness of a variety of threats, he refrains from embracing any wide-reaching explanation. It can be argued that the constant message of impending destruction is simply a way for the media to keep us watching television—“*Are cyber predators targeting your children?*” is a tagline that is going to get the audience's attention. What interests me is not the reality of these threats, but the effect they have on our view of the world.

Fear encourages intolerance, racism and xenophobia. Fear creates the need for a constant series of symbolic actions manufactured by the authorities to show that—yes, they are protecting us from all possible dangers.

In “The Traveler,” powerful men use fear to keep the population under control. While I don't believe that a shadowy group of Illuminati are guiding the industrial world, I think it's clear that a variety of institutions use fear to manipulate public opinion.

Awareness of the past seems ever less important as history is superseded by the present crisis. Most people can still recall the so-called Weapons of Mass Destruction used to justify the war in Iraq, but the fact that the WMD never existed seems to have disappeared from the day-to-day public discourse. We simply moved on—to a new threat.

Many of our leaders have gone past the old-fashioned politics of the democratic era and entered into the politics of fear. People running for national office no longer emphasize their view of economics or social change. The leading political question of our time has become: who can ease our nightmares? We are being watched and controlled without our knowledge, but the biggest surprise is that there is little broad-based objection to this significant change in our society. Instead of resisting the Vast Machine, many of us have given into cynicism and distraction. Our contemporary culture has become a brilliantly colored surface without a deeper spiritual meaning.

We care more about celebrities than our own neighbors. Are Nick and Jessica getting divorced? Is that famous actor secretly gay? Staged media events allow us to think that everything is false.

Our sense of powerlessness—the belief that an ordinary person does not matter—has twisted our lips into a sneer.

Although I recognize the growing reality of the Vast Machine, I refuse to accept its authority. Each one of us needs to make a choice about what kind of world we want in the future.

The pose of rebellion based on style and attitude is an empty gesture. Political affiliation is not a relevant part of this decision; privacy and personal freedom should be fundamental right for everyone.

The first step is awareness: the realization we are being monitored without our consent.

When we use a shopping card, there's no need to also include accurate data in the application.

Why should our desire to get a discount on detergent require us to provide our address, our phone number and other personal data? All of us need to protect our home computers with programs that destroy spyware. We should realize the implications of giving our social

[We Speak for Freedom](http://wespeakforfreedom.com)

<http://wespeakforfreedom.com>

security numbers to large corporations. In real life, protecting one's privacy is never a single dramatic action; it's based on adopting a new attitude toward the powerful forces that want to reduce our lives to a digital image.

We have the power to resist the constant message of fear.

We have the power to use technology, not as a means of control, but as a tool to improve our own society.

In my novel, people are waiting for a Traveler, a visionary, to emerge from the darkness and change their lives. The Travelers are almost extinct, and the last few are defended by a small group of fighters called Harlequins. A great battle has started that will be described in the next two books of the trilogy.

In the real world, our battle will be made of small gestures—small decisions—to protect our private selves from the intrusions of the Vast Machine. No outside force will save us. We must look into our own hearts to find the Travelers and Harlequins—the prophets and warriors—who will keep us free.