

1 of 1 DOCUMENT

Copyright 2001 The New York Times Company  
The New York TimesOctober 7, 2001 Sunday  
Late Edition - Final**SECTION:** Section 6; Column 1; Magazine Desk; Pg. 38**LENGTH:** 6127 words**HEADLINE:** A Watchful State**BYLINE:** By Jeffrey Rosen; Jeffrey Rosen is an associate professor at George Washington University Law School and the legal affairs editor of The New Republic. He writes frequently on law for The Times Magazine.**BODY:**

A week after the attacks of Sept. 11, as the value of most American stocks plummeted, a few companies, with products particularly well suited for a new and anxious age, soared in value. One of the fastest growing stocks was Visionics, whose price more than tripled. The New Jersey company is an industry leader in the fledgling science of biometrics, a method of identifying people by scanning and quantifying their unique physical characteristics — their facial structures, for example, or their retinal patterns. Visionics manufactures a face-recognition technology called FaceIt, which creates identification codes for individuals based on 80 unique aspects of their facial structures, like the width of the nose and the location of the temples. FaceIt can instantly compare an image of any individual's face with a database of the faces of suspected terrorists, or anyone else.

Visionics was quick to understand that the terrorist attacks represented not only a tragedy but also a business opportunity. On the afternoon of Sept. 11, the company sent out an e-mail message to reporters, announcing that its founder and C.E.O., Joseph Atick, "has been speaking worldwide about the need for biometric systems to catch known terrorists and wanted criminals." On Sept. 20, Atick testified before a special government committee appointed by the secretary of transportation, Norman Mineta. Atick's message — that security in airports and embassies could be improved using face-recognition technology as part of a comprehensive national surveillance plan that he called Operation Noble Shield — was greeted enthusiastically by members of the committee, which seemed ready to endorse his recommendations. "In the war against terrorism, especially when it comes to the homeland defense," Atick told me, describing his testimony, "the cornerstone of this is going to be our ability to identify the enemy before he or she enters into areas where public safety could be at risk."

Atick proposes to wire up Reagan National Airport in Washington and other vulnerable airports throughout the country with more than 300 cameras each. Cameras would scan the faces of passengers standing in line, and biometric technology would be used to analyze their faces and make sure they are not on an international terrorist "watch list." More cameras unobtrusively installed throughout the airport could identify passengers as they walk through metal detectors and public areas. And a final scan could ensure that no suspected terrorist boards a plane. "We have created a biometric network platform that turns every camera into a Web browser submitting images to a database in Washington, querying for matches," Atick said. "If a match occurs, it will set off an alarm in Washington, and someone will make a decision to wire the image to marshals at the airport."

Of course, protecting airports is only one aspect of homeland security: a terrorist could be lurking on any corner in America. In the wake of the Sept. 11 attacks, Howard Safir, the former New York police commissioner, recommended the installation of 100 biometric surveillance cameras in Times Square to scan the faces of pedestrians and compare them with a database of suspected terrorists. Atick told me that since the attacks he has been approached by local and federal authorities from across the country about the possibility of installing biometric surveillance cameras in stadiums and subway systems and near national monuments. "The Office of Homeland Security might be the overall umbrella that will coordinate with local police forces" to install cameras linked to a biometric network throughout American cities, Atick told me. "How can we be alerted when someone is entering the subway? How can we be sure when someone is entering

Madison Square Garden? How can we protect monuments? We need to create an invisible fence, an invisible shield."

Before Sept. 11, the idea that Americans would voluntarily agree to live their lives under the gaze of a network of biometric surveillance cameras, peering at them in government buildings, shopping malls, subways and stadiums, would have seemed unthinkable, a dystopian fantasy of a society that had surrendered privacy and anonymity. But in fact, over the past decade, this precise state of affairs has materialized, not in the United States but in the United Kingdom. At the beginning of September, as it happened, I was in Britain, observing what now looks like a glimpse of the American future.

I had gone to Britain to answer a question that seems far more pertinent today than it did early last month: why would a free and flourishing Western democracy wire itself up with so many closed-circuit television cameras that it resembles the set of "The Real World" or "The Truman Show"? The answer, I discovered, was fear of terrorism. In 1993 and 1994, two terrorist bombs planted by the I.R.A. exploded in London's financial district, a historic and densely packed square mile known as the City of London. In response to widespread public anxiety about terrorism, the government decided to install a "ring of steel" — a network of closed-circuit television cameras mounted on the eight official entry gates that control access to the City.

Anxiety about terrorism didn't go away, and the cameras in Britain continued to multiply. In 1994, a 2-year-old boy named Jamie Bulger was kidnapped and murdered by two 10-year-old schoolboys, and surveillance cameras captured a grainy shot of the killers leading their victim out of a shopping center. Bulger's assailants couldn't, in fact, be identified on camera — they were caught because they talked to their friends — but the video footage, replayed over and over again on television, shook the country to its core. Riding a wave of enthusiasm for closed-circuit television, or CCTV, created by the attacks, John Major's Conservative government decided to devote more than three-quarters of its crime-prevention budget to encourage local authorities to install CCTV. The promise of cameras as a magic bullet against crime and terrorism inspired one of Major's most successful campaign slogans: "If you've got nothing to hide, you've got nothing to fear."

Instead of being perceived as an Orwellian intrusion, the cameras in Britain proved to be extremely popular. They were hailed as the people's technology, a friendly eye in the sky, not Big Brother at all but a kindly and watchful uncle or aunt. Local governments couldn't get enough of them; each hamlet and fen in the British countryside wanted its own CCTV surveillance system, even when the most serious threat to public safety was coming from mad cows. In 1994, 79 city centers had surveillance networks; by 1998, 440 city centers were wired. By the late 1990's, as part of its Clintonian, center-left campaign to be tough on crime, Tony Blair's New Labor government decided to support the cameras with a vengeance. There are now so many cameras attached to so many different surveillance systems in the U.K. that people have stopped counting. According to one estimate, there are 2.5 million surveillance cameras in Britain, and in fact there may be far more.

As I filed through customs at Heathrow Airport, there were cameras concealed in domes in the ceiling. There were cameras pointing at the ticket counters, at the escalators and at the tracks as I waited for the Heathrow express to Paddington Station. When I got out at Paddington, there were cameras on the platform and cameras on the pillars in the main terminal. Cameras followed me as I walked from the main station to the underground, and there were cameras at each of the stations on the way to King's Cross. Outside King's Cross, there were cameras trained on the bus stand and the taxi stand and the sidewalk, and still more cameras in the station. There were cameras on the backs of buses to record people who crossed into the wrong traffic lane.

Throughout Britain today, there are speed cameras and red-light cameras, cameras in lobbies and elevators, in hotels and restaurants, in nursery schools and high schools. There are even cameras in hospitals. (After a raft of "baby thefts" in the early 1990's, the government gave hospitals money to install cameras in waiting rooms, maternity wards and operating rooms.) And everywhere there are warning signs, announcing the presence of cameras with a jumble of different icons, slogans and exhortations, from the bland "CCTV in operation" to the peppy "CCTV: Watching for You!" By one estimate, the average Briton is now photographed by 300 separate cameras in a single day.

Britain's experience under the watchful eye of the CCTV cameras is a vision of what Americans can expect if we choose to go down the same road in our efforts to achieve "homeland security." Although the cameras in Britain were initially justified as a way of combating terrorism, they soon came to serve a very different function. The cameras are designed not to produce arrests but to make people feel that they are being watched at all times. Instead of keeping terrorists off planes, biometric surveillance is being used to keep punks out of shopping malls. The people behind the live video screens are zooming in on unconventional behavior in public that in fact has nothing to do with terrorism. And

rather than thwarting serious crime, the cameras are being used to enforce social conformity in ways that Americans may prefer to avoid.

The dream of a biometric surveillance system that can identify people's faces in public places and separate the innocent from the guilty is not new. Clive Norris, a criminologist at the University of Hull, is Britain's leading authority on the social effects of CCTV. In his definitive study, "The Maximum Surveillance Society: the Rise of CCTV," Norris notes that in the 19th century, police forces in England and France began to focus on how to distinguish the casual offender from the "habitual criminal" who might evade detection by moving from town to town. In the 1870's, Alphonse Bertillon, a records clerk at the prefecture of police in Paris, used his knowledge of statistics and anthropomorphic measurements to create a system for comparing the thousands of photographs of arrested suspects in Parisian police stations. He took a series of measurements — of skull size, for example, and the distance between the ear and chin — and created a unique code for every suspect whom the police had photographed. Photographs were then grouped according to the codes, and a new suspect could be compared only with the photos that had similar measurements, instead of with the entire portfolio. Though Bertillon's system was often difficult for unskilled clerks to administer, a procedure that had taken hours or days was now reduced to a few minutes.

It wasn't until the 1980's, with the development of computerized biometric and other face-recognition systems, that Bertillon's dream became feasible on a broad scale. In the course of studying how biometric scanning could be used to authenticate the identities of people who sought admission to secure buildings, innovators like Joseph Atick realized that the same technology could be used to pick suspects or license plates out of a crowd. It's the license-plate technology that the London police have found most attractive, because it tends to be more reliable. (A test of the best face-recognition systems last year by the U.S. Department of Defense found that they failed to identify matches a third of the time.)

Soon after arriving in London, I visited the CCTV monitoring room in the City of London police station, where the British war against terrorism began. I was met by the press officer, Tim Parsons, and led up to the control station, a modest-size installation that looks like an air-traffic-control room, with uniformed officers manning two rows of monitors. Although installed to catch terrorists, the cameras in the City of London spend most of their time following car thieves and traffic offenders. "The technology here is geared up to terrorism," Parsons told me. "The fact that we're getting ordinary people — burglars stealing cars — as a result of it is sort of a bonus."

Have you caught any terrorists? I asked. "No, not using this technology, no," he replied.

As we watched the monitors, rows of slow-moving cars filed through the gates into the City, and cameras recorded their license-plate numbers and the faces of their drivers. After several minutes, one monitor set off a soft, pinging alarm. We had a match! But no, it was a false alarm. The license plate that set off the system was 8620bmc, but the stolen car recorded in the database was 8670amc. After a few more mismatches, the machine finally found an offender, though not a serious one. A red van had gone through a speed camera, and the local authority that issued the ticket couldn't identify the driver. An alert went out on the central police national computer, and it set off the alarm when the van entered the City. "We're not going to do anything about it because it's not a desperately important call," said the sergeant.

Because the cameras on the ring of steel take clear pictures of each driver's face, I asked whether the City used the biometric facial recognition technology that American airports are now being urged to adopt. "We're experimenting with it to see if we could pick faces out of the crowd, but the technology is not sufficiently good enough," Parsons said. "The system that I saw demonstrated two or three years ago, a lot of the time it couldn't differentiate between a man and a woman." (In a recent documentary about CCTV, Monty Python's John Cleese foiled a Visionics face-recognition system that had been set up in the London borough of Newham by wearing earrings and a beard.) Nevertheless, Parsons insisted that the technology will become more accurate. "It's just a matter of time. Then we can use it to detect the presence of criminals on foot in the city," he said.

In the future, as face-recognition technology becomes more accurate, it will become even more intrusive, because of pressures to expand the biometric database. I mentioned to Joseph Atick of Visionics that the City of London was thinking about using his technology to establish a database that would include not only terrorists but also all British citizens whose faces were registered with the national driver's license bureau. If that occurs, every citizen who walks the streets of the City could be instantly identified by the police and evaluated in light of his past misdeeds, no matter how trivial. With the impatience of a rationalist, Atick dismissed the possibility. "Technically, they won't be able to do it without coming back to me," he said. "They will have to justify it to me." Atick struck me as a refined and thoughtful man (he is the former director of the computational neuroscience laboratory at Rockefeller University), but it seems odd to put the liberties of a

democracy in the hands of one unelected scientist.

Atick says that his technology is an enlightened alternative to racial and ethnic profiling, and if the faces in the biometric database were, in fact, restricted to known terrorists, he would be on to something. Instead of stopping all passengers who appear to be Middle Eastern and victimizing thousands of innocent people, the system would focus with laserlike precision on a tiny handful of the guilty. (This assumes that the terrorists aren't cunning enough to disguise themselves.) But when I asked whether any of the existing biometric databases in England or America are limited to suspected terrorists, Atick confessed that they aren't. There is a simple reason for this: few terrorists are suspected in advance of their crimes. For this reason, cities in England and elsewhere have tried to justify their investment in face-recognition systems by filling their databases with those troublemakers whom the authorities can easily identify: local criminals. When FaceIt technology was used to scan the faces of the thousands of fans entering the Super Bowl in Tampa last January, the matches produced by the database weren't terrorists. They were low-level ticket scalpers and pickpockets.

Biometrics is a feel-good technology that is being marketed based on a false promise — that the database will be limited to suspected terrorists. But the FaceIt technology, as it's now being used in England, isn't really intended to catch terrorists at all. It's intended to scare local hoodlums into thinking they might be setting off alarms even when the cameras are turned off. I came to understand this "Wizard of Oz" aspect of the technology when I visited Bob Lack's monitoring station in the London borough of Newham. A former London police officer, Lack attracted national attention — including a visit from Tony Blair — by pioneering the use of face-recognition technology before other people were convinced that it was entirely reliable. What Lack grasped early on was that reliability was in many ways beside the point.

Lack installed his first CCTV system in 1997, and he intentionally exaggerated its powers from the beginning. "We put one camera out and 12 signs" announcing the presence of cameras, Lack told me. "We reduced crime by 60 percent in the area where we posted the signs. Then word on the street went out that we had dummy cameras." So Lack turned his attention to face-recognition technology and tried to create the impression that far more people's faces were in the database than actually are. "We've designed a poster now about making Newham a safe place for a family," he said. "And we're telling the criminal we have this information on him: we know his name, we know his address, we know what crimes he commits." It's not true, Lack admits, "but then, we're entitled to disinform some people, aren't we?"

So you're telling the criminal that you know his name even though you don't, I asked? "Right," Lack replied. "Pretty much that's about advertising, isn't it?"

Lack was elusive when I asked him who, exactly, is in his database. "I don't know," he replied, noting that the local police chief decides who goes into the database. He would only make an "educated guess" that the database contains 100 "violent street robbers" under the age of 18. "You have to have been convicted of a crime — nobody suspected goes on, unless they're a suspected murderer — and there has to be sufficient police intelligence to say you are committing those crimes and have been so in the last 12 weeks." When I asked for the written standards that determined who, precisely, was put in the database, and what crimes they had to have committed, Lack promised to send them, but he never did.

From Lack's point of view, it doesn't matter who is in his database, because his system isn't designed to catch terrorists or violent criminals. In the three years that the system has been up and running, it hasn't resulted in a single arrest. "I'm not in the business of having people arrested," Lack said. "The deterrent value has far exceeded anything you imagine." He told me that the alarms went off an average of three times a day during the month of August, but the only people he would conclusively identify were local youths who had volunteered to be put in the database as part of an "intensive surveillance supervision program," as an alternative to serving a custodial sentence. "The public statements about the efficacy of the Newham facial-recognition system bear little relationship to its actual operational capabilities, which are rather weak and poor," says Clive Norris of the University of Hull. "They want everyone to believe that they are potentially under scrutiny. Its effectiveness, perhaps, is based on a lie."

This lie has a venerable place in the philosophy of surveillance. In his preface to "Panopticon," Jeremy Bentham imagined the social benefits of a ring-shaped "inspection-house," in which prisoners, students, orphans or paupers could be subject to constant surveillance. In the center of the courtyard would be an inspection tower with windows facing the inner wall of the ring. Supervisors in the central tower could observe every movement of the inhabitants of the cells, who were illuminated by natural lighting, but Venetian blinds would ensure that the supervisors could not be seen by the inhabitants. The uncertainty about whether or not they were being surveilled would deter the inhabitants from antisocial behavior. Michel Foucault described the purpose of the Panopticon — to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power." Foucault predicted that this condition of visible,

unverifiable power, in which individuals have internalized the idea that they may always be under surveillance, would be the defining characteristic of the modern age.

Britain, at the moment, is not quite the Panopticon, because its various camera networks aren't linked and there aren't enough operators to watch all the cameras. But over the next few years, that seems likely to change, as Britain moves toward the kind of integrated Web-based surveillance system that Visionics has now proposed for American airports and subway systems. At the moment, for example, the surveillance systems for the London underground and the British police feed into separate control rooms, but Sergio Velastin, a computer-vision scientist, says he believes the two systems will eventually be linked, using digital technology.

Velastin is working on behavioral-recognition technology for the London underground that can look for unusual movements in crowds, setting off an alarm, for example, when people appear to be fighting or trying to jump on the tracks. (Because human CCTV operators are easily bored and distracted, automatic alarms are viewed as the wave of the future.) "Imagine you see a piece of unattended baggage which might contain a bomb," Velastin told me. "You can back-drag on the image and locate the person who left it there. You can say where did that person come from and where is that person now? You can conceive in the future that you might be able to do that for every person in every place in the system." Of course, Velastin admitted, "if you don't have social agreement about how you're going to operate that, it could get out of control."

Once thousands of cameras from hundreds of separate CCTV systems are able to feed their digital images to a central monitoring station, and the images can be analyzed with face-and behavioral-recognition software to identify unusual patterns, then the possibilities of the Panopticon will suddenly become very real. And few people doubt that connectivity is around the corner; it is, in fact, the next step. "CCTV will become the fifth utility: after gas, electricity, sewage and telecommunications," says Jason Ditton, a criminologist at the University of Sheffield who is critical of the technology's expansion. "We will come to accept its ubiquitousness."

At the moment, there is only one fully integrated CCTV in Britain: it transmits digital images over a broadband wireless network, like the one Joseph Atick has proposed for American airports, rather than relying on traditional video cameras that are chained to dedicated cables. And so, for a still clearer vision of the interconnected future of surveillance, I set off for Hull, Britain's leading timber port, about three hours northeast of London. Hull has traditionally been associated not with dystopian fantasies but with fantasies of a more basic sort: for hundreds of years, it has been the prostitution capital of northeastern Britain.

Six years ago, a heroin epidemic created an influx of addicted young women who took to streetwalking to sustain their drug habit. Nearly two years ago, the residents' association of a low-income housing project called Goodwin Center hired a likable and enterprising young civil engineer named John Marshall to address the problem of under-age prostitutes having sex on people's windowsills.

Marshall, who is now 33, met me at the Hull railway station carrying a CCTV warning sign. Armed with more than a million dollars in public financing from the European Union, Marshall decided to build what he calls the world's first Ethernet-based, wireless CCTV system. Initially, Marshall put up 27 cameras around the housing project. The cameras didn't bother the prostitutes, who in fact felt safer working under CCTV. Instead, they scared the johns — especially after the police recorded their license numbers, banged on their doors and threatened to publish their names in the newspapers. Business plummeted, and the prostitutes moved indoors or across town to the traditional red-light district, where the city decided to tolerate their presence in limited numbers.

But Marshall soon realized that he had bigger fish to fry than displacing prostitutes from one part of Hull to another. His innovative network of linked cameras attracted national attention, which led, a few months ago, to \$20 million in grant money from various levels of government to expand the surveillance network throughout the city of Hull. "In a year and a half," Marshall says, "there'll be a digital connection to every household in the city. As far as cameras go, I can imagine that, in 10 years' time, the whole city will be covered. That's the speed that CCTV is growing." In the world that Marshall imagines, every household in Hull will be linked to a central network that can access cameras trained inside and outside every building in the city. "Imagine a situation where you've got an elderly relative who lives on the other side of the city," Marshall says. "You ring her up, there's no answer on the telephone, you think she collapsed — so you go to the Internet and you look at the camera in the lounge and you see that she's making a cup of tea and she's taken her hearing aid out or something."

The person who controls access to this network of intimate images will be a very powerful person indeed. And so I

was eager to meet the monitors of the Panopticon for myself. On a side street of Hull, near the Star and Garter Pub and the city morgue, the Goodwin Center's monitoring station is housed inside a ramshackle private security firm called Sentry Alarms Ltd. The sign over the door reads THE GUARD HOUSE. The monitoring station is locked behind a thick, black vault-style door, but it looks like a college computer center, with an Alicia Silverstone pinup near the door. Instead of an impressive video wall, there are only two small desktop computers, which receive all the signals from the Goodwin Center network. And the digital, Web-based images — unlike traditional video — are surprisingly fuzzy and jerky, like streaming video transmitted over a slow modem.

During my time in the control room, from 9 p.m. to midnight, I experienced firsthand a phenomenon that critics of CCTV surveillance have often described: when you put a group of bored, unsupervised men in front of live video screens and allow them to zoom in on whatever happens to catch their eyes, they tend to spend a fair amount of time leering at women. "What catches the eye is groups of young men and attractive, young women," I was told by Clive Norris, the Hull criminologist. "It's what we call a sense of the obvious." There are plenty of stories of video voyeurism: a control room in the Midlands, for example, took close-up shots of women with large breasts and taped them up on the walls. In Hull, this temptation is magnified by the fact that part of the operators' job is to keep an eye on prostitutes. As it got late, though, there weren't enough prostitutes to keep us entertained, so we kept ourselves awake by scanning the streets in search of the purely consensual activities of boyfriends and girlfriends making out in cars. "She had her legs wrapped around his waist a minute ago," one of the operators said appreciatively as we watched two teenagers go at it. "You'll be able to do an article on how reserved the British are, won't you?" he joked. Norris also found that operators, in addition to focusing on attractive young women, tend to focus on young men, especially those with dark skin. And those young men know they are being watched: CCTV is far less popular among black men than among British men as a whole. In Hull and elsewhere, rather than eliminating prejudicial surveillance and racial profiling, CCTV surveillance has tended to amplify it.

After returning from the digital city of Hull, I had a clearer understanding of how, precisely, the spread of CCTV cameras is transforming British society and why I think it's important for America to resist going down the same path. "I actually don't think the cameras have had much effect on crime rates," says Jason Ditton, the criminologist, whose evaluation of the effect of the cameras in Glasgow found no clear reduction in violent crime. "We've had a fall in crime in the last 10 years, and CCTV proponents say it's because of the cameras. I'd say it's because we had a boom economy in the last seven years and a fall in unemployment." Ditton notes that the cameras can sometimes be useful in investigating terrorist attacks — like the Brixton nail-bomber case in 1999 — but there is no evidence that they prevent terrorism or other serious crime.

Last year, Britain's violent crime rates actually increased by 4.3 percent, even though the cameras continued to proliferate. But CCTV cameras have a mysterious knack for justifying themselves regardless of what happens to crime. When crime goes up the cameras get the credit for detecting it, and when crime goes down, they get the credit for preventing it.

If the creation of a surveillance society in Britain hasn't prevented terrorist attacks, it has had subtle but far-reaching social costs. The handful of privacy advocates in Britain have tried to enumerate those costs by arguing that the cameras invade privacy. People behave in self-conscious ways under the cameras, ostentatiously trying to demonstrate their innocence or bristling at the implication of guilt. Inside a monitoring room near Runnymede, the birthplace of the Magna Carta, I saw a group of teenagers who noticed that a camera was pivoting around to follow them; they made an obscene gesture toward it and looked back over their shoulders as they tried to escape its gaze.

The cameras are also a powerful inducement toward social conformity for citizens who can't be sure whether they are being watched. "I am gay and I might want to kiss my boyfriend in Victoria Square at 2 in the morning," a supporter of the cameras in Hull told me. "I would not kiss my boyfriend now. I am aware that it has altered the way I might behave. Something like that might be regarded as an offense against public decency. This isn't San Francisco." Nevertheless, the man insisted that the benefits of the cameras outweighed the costs, because "thousands of people feel safer."

There is, in the end, a powerfully American reason to resist the establishment of a national surveillance network: the cameras are not consistent with the values of an open society. They are technologies of classification and exclusion. They are ways of putting people in their place, of deciding who gets in and who stays out, of limiting people's movement and restricting their opportunities. I came to appreciate the exclusionary potential of the surveillance technology in a relatively low-tech way when I visited a shopping center in Uxbridge, a suburb of London. The manager of the center explained that people who are observed to be misbehaving in the mall can be banned from the premises. The banning process isn't very complicated. "Because this isn't public property, we have the right to refuse entry, and if there's a wrongdoer, we give

them a note or a letter, or simply tell them you're banned." In America, this would provoke anyone who was banned to call Alan Dershowitz and sue for discrimination. But the British are far less litigious and more willing to defer to authority.

Banning people from shopping malls is only the beginning. A couple of days before I was in London, Borders Books announced the installation of a biometric face-recognition surveillance system in its flagship store on Charing Cross Road. Borders' scheme meant that anyone who had shoplifted in the past was permanently branded as a shoplifter in the future. In response to howls of protest from America, Borders dismantled the system, but it may well be resurrected in a post-Sept. 11 world.

Perhaps the reason that Britain has embraced the new technologies of surveillance, while America, at least before Sept. 11, had strenuously resisted them, is that British society is far more accepting of social classifications than we are. The British desire to put people in their place is the central focus of British literature, from Dickens to John Osborne and Alan Bennett. The work of George Orwell that casts the most light on Britain's swooning embrace of CCTV is not "1984." It is Orwell's earlier book "The English People."

"Exaggerated class distinctions have been diminishing," Orwell wrote, but "the great majority of the people can still be 'placed' in an instant by their manners, clothes and general appearance" and above all, their accents. Class distinctions are less hardened today than they were when I was a student at Oxford at the height of the Thatcher-era "Brideshead Revisited" chic. But it's no surprise that a society long accustomed to the idea that people should know their place didn't hesitate to embrace a technology designed to ensure that people stay in their assigned places.

Will America be able to resist the pressure to follow the British example and wire itself up with surveillance cameras? Before Sept. 11, I was confident that we would. Like Germany and France, which are squeamish about CCTV because of their experience with 20th-century totalitarianism, Americans are less willing than the British to trust the government and defer to authority. After Sept. 11, however, everything has changed. A New York Times/CBS news poll at the end of September found that 8 in 10 Americans believe they will have to give up some of their personal freedoms to make the country safe from terrorist attacks.

Of course there are some liberties that should be sacrificed in times of national emergency if they give us greater security. But Britain's experience in the fight against terrorism suggests that people may give up liberties without experiencing a corresponding increase in security. And if we meekly accede in the construction of vast feel-good architectures of surveillance that have far-reaching social costs and few discernible social benefits, we may find, in calmer times, that they are impossible to dismantle.

It's important to be precise about the choice we are facing. No one is threatening at the moment to turn America into Orwell's Big Brother. And Britain hasn't yet been turned into Big Brother, either. Many of the CCTV monitors and camera operators and policemen and entrepreneurs who took the time to meet with me were models of the British sense of fair play and respect for the rules. In many ways, the closed-circuit television cameras have only exaggerated the qualities of the British national character that Orwell identified in his less famous book: the acceptance of social hierarchy combined with the gentleness that leads people to wait in orderly lines at taxi stands; a deference to authority combined with an appealing tolerance of hypocrisy. These English qualities have their charms, but they are not American qualities.

The promise of America is a promise that we can escape from the Old World, a world where people know their place. When we say we are fighting for an open society, we don't mean a transparent society — one where neighbors can peer into each other's windows using the joysticks on their laptops. We mean a society open to the possibility that people can redefine and reinvent themselves every day; a society in which people can travel from place to place without showing their papers and being encumbered by their past; a society that respects privacy and constantly reshuffles social hierarchy.

The ideal of America has from the beginning been an insistence that your opportunities shouldn't be limited by your background or your database; that no doors should be permanently closed to anyone who has the wrong smart card. If the 21st century proves to be a time when this ideal is abandoned — a time of surveillance cameras and creepy biometric face scanning in Times Square — then Osama bin Laden will have inflicted an even more terrible blow than we now imagine.

**URL:** <http://www.nytimes.com>

**GRAPHIC:** Photos: Surveillance images from cameras in London's financial district. Britain has redefined reality TV.; Stolen Kiss: Surveillance cameras like this one in London capture criminals and noncriminals alike.; Warning Signs: Throughout London, there are reminders of the cameras' presence. (Stephen Gill)