Liberty in the age of technology

Increasing government surveillance worldwide raises tough questions for democracy and civil liberty. Left unchecked, the deployment of intrusive new technologies poses a profound threat to individual privacy. What we need, says **Barry Steinhardt**, is stronger regulation to ensure that such technology is used fairly – by governments and businesses alike

The vision of the future portrayed in Steven Spielberg's recent hit film *Minority Report* is ostensibly a work of Hollywood fantasy.

Set in the year 2053, its protagonist Paul Anderton is on the run – fleeing a police force armed with an overpowering array of technology to hunt down their villain. Anderton is identified and tracked down with striking precision thanks his adversaries' high-tech gadgetry.

But the surveillance technologies portrayed in this film are all too chillingly real. They are either already in existence or coming soon, for use by the government and the private sector alike.

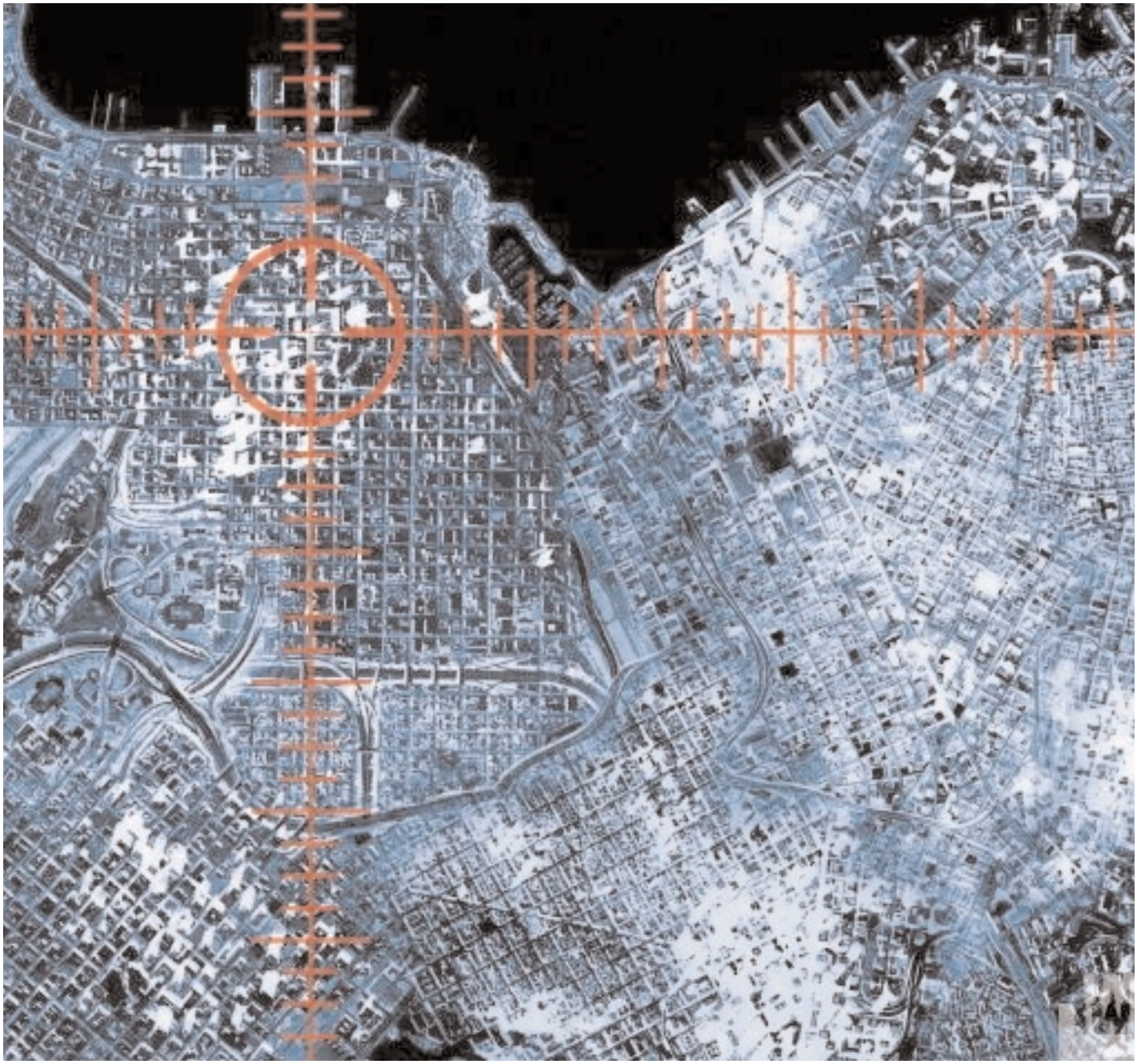
Among the sundry devices on offer in the film is "thermal imaging," although admittedly in this case it is deployed by spider-like robots equipped with the imaging technologies. But Anderton is also identified with a scan of his eye and is then pursued by a simple check of a powerful database that is present not only in high-security locations, but also in his car. It's even active as he walks through a shopping mall.

In truth, the surveillance equipment portrayed in *Minority Report* is modest compared with what is already possible. For example, much attention recently has focused on radio frequency identity chips (RFIDs) that can be implanted in both people and objects to allow them to be monitored and identified.

But RFID chips are just a small part of a much larger mosaic of surveillance tools. Powerful cameras, sensors, communication monitoring capabilities, global positioning satellite technology and biometrics are feeding a surveillance monster that is growing silently in our midst. And scarcely a month goes by in which we don't read about some new high-tech method for tracking and identifying us.

In fact there are no longer any technical barriers to the kind of Big Brother surveillance society envisioned by George Orwell – or, more recently, Spielberg. The barriers that remain are political and legal.

We should be responding to intrusive new technologies by building stronger restraints to protect our privacy. Unfortunately, in the United States we are doing the opposite – loosening regulations on government surveillance, watching passively as private surveillance grows unchecked, and contemplating the introduction



THE IMAGE BANK (digital composite)

There are no longer any technical barriers to the kind of Big Brother surveillance society envisaged by George Orwell

of tremendously powerful new surveillance infrastructures like the Total Information Awareness programme that will tie all this information together

For good or ill?

The private sector will play a significant role in this unfolding story, whether for good or for ill. In the short run, government surveillance requirements are placing an enormous financial burden on the business community.

In the United States for example, the Communications Assistance to Law Enforcement Act is forcing telecommunications providers to spend billions of dollars to design their equipment to enable eavesdropping.

Internet service providers (ISPs) report that search orders and other government requests for information have increased dramatically. Private companies – from banks, to health insurers, to pawn brokers – are being forced to develop expensive systems for sending records of their customers' suspicious transactions to a central government repository.

The *Atlanta Business Chronicle* reported in November 2002 that Bank of America was forced to create a whole new department to handle the government's new surveillance mandates. These workers are, in effect, outsourced employees of the government's growing surveillance machine.

An even wider segment of the business community will soon be experiencing this phenomenon as the federal government makes use of its newly enhanced power to issue "National Security Letters". These are demands for data that require neither a warrant reviewed by an independent judge nor extensive justification.

On the other hand, other businesses, from the burgeoning biometrics industry to information aggregators and brokers, are actively pushing for expanded government monitoring. Ironically this burgeoning surveillance-industrial complex will not make us any safer. It will just make us less free.

A congressional investigation into the September 11 terrorist attacks found that the government's failure to prevent the attacks was not caused by a shortage of cutting-edge surveillance technology.

Rather, it was the result of fundamental organizational breakdowns in the intelligence com-

munity, and the government's failure to make effective use of the surveillance powers it already had.

But regrettably, too many US companies have found that there is more money to be made providing technologies that offer only the illusion of security, than there is in sorting out bureaucracies, fixing institutional cultures, or addressing fundamental security problems such as passenger baggage-matching (recognized around the world as a basic security step, but opposed by US carriers for economic reasons, and therefore not required in the United States).

An international problem

The growing potential for sharply increased government surveillance is a problem not just in the United States, but in every advanced nation. The United Kingdom, in particular, has arguably travelled the furthest among all nations towards a total surveillance society.

Among other developments, it has deployed the most pervasive network of police-operated video cameras on earth. It is has the most complete database of DNA – the very stuff of life that harbours our most intimate secrets – of any large industrialized nation. The United Kingdom is now in the process of creating a biometric-laden identity card – and there is even talk of tying it to the DNA database.

While Europe as a whole has sought to place chains on the surveillance monster through the European Union's overarching Data Protection Directive, and with the fundamental privacy protections in the European Convention on Human Rights (ECHR), those chains are beginning to weaken.

To America's shame, many of these assaults on privacy – not just in Europe, but around the world – have come at the instigation of the United States. While US privacy activists always hoped that the existence of strong privacy laws in the rest of the developed world would rub off on the legal regime that prevails in the United States, the influence so far appears to be moving in the other direction.

Indeed, the US government frequently appears to be engaging in a strategy of "policy laundering" – furthering anti-privacy policy goals by forcing them on our allies or on international institutions.

> Private companies – from banks, to health insurers, to pawn brokers – are being forced to develop expensive systems for sending records of their customers' suspicious transactions to a central government repository

> RFID chips are just a part of a much larger mosaic of surveillance tools. Powerful cameras, sensors, communication monitoring capabilities, GPS technology and biometrics are feeding a surveillance monster that is growing silently in our midst

The United States is successfully pressuring its allies to put biometrics on identity documents by threatening to revoke their citizens' right to no-visa US travel if they do not implement the technology by October 2004.

Britain, and the European Union as a whole, has moved in that direction – and not just for travel documents, but for all identity cards.

At the not-particularly-subtle instigation of the United States, governments in Europe and elsewhere have begun to turn their ISPs and other telecommunications companies into surveillance agents by forcing them to retain, and share with the government, data on customers' phone calls, emails and web surfing.

As was noted during a contentious debate in Britain's House of Lords recently, forced data retention almost certainly contravenes Article 8 of the ECHR.

But there is something even more fundamental at play – a dramatic shift in the understanding of the proper role of government in a democratic society. In Europe's case, it brings to mind its darkest days.

"This goes to the very root of a democratic society," Brandenburg commissioner for data protection Alexander Dix said after German interior minister Otto Schily proposed that communications data be stored by German internet service providers.

He went on: "Telecommunications secrecy is very strongly enshrined in our constitution. The Gestapo experience and also the Stasi experience are something which are very present in the public mind here."

A stage set for clashes

The existence of these laws and experiences in Europe has set the stage for clashes as the US law enforcement and national security establishments push to extend the tentacles of surveillance to draw in visitors and potential visitors as well as residents.

The EU data directive, for example, prohibits the export of personal information to countries that do not themselves have sufficient privacy standards (a straightforward measure made necessary to avoid opening up a giant loophole in the rules). Unfortunately, the United States belongs in that category.

One result is that the United States has encountered stiff opposition from some elements in the European Union (most notably the parliament and data commissioners) in its attempts to implement a profiling and background-check system for airline passengers, known as CAPPS II.

This programme would carry out computerized background checks on every person who flies, and use a secret process based on secret sources of information to rate their risk to air safety – all with no meaningful due process mechanisms to ensure fairness.

US and EU negotiators are still negotiating over US demands for sensitive personal information about Europeans flying to the States. The United States wants a broad range of information about each traveller.

Even before the system has been built, the government is proclaiming the right to use that information not just for anti-terrorism purposes, but for ordinary law enforcement and possibly even for the enforcement of immigration laws.

This has created an untenable situation in which the US government must force Europeans to violate their own laws, or accede to the European laws and treat European visitors better than it does its own citizens.

The role that European privacy laws, like the data directive, and institutional forces, like the privacy commissioners, have played in slowing the rush towards a surveillance society demonstrates that chains can be placed on the monster.

But unceasing vigilance and constant will is necessary to maintain those chains, particularly in times of crisis like those we face post September 11.

Steven Spielberg's Paul Anderton never tried to leave the United States. But if current trends continue, in the year 2053 we, like Anderton, will find ourselves under legalized surveillance no matter where in the world we go. GA

CV BARRY STEINHARDT

Barry Steinhardt is the director of the Programme on Technology and Liberty at the American Civil Liberties Union . He has been associate director of ACLU for the past 10 years. He was a co-founder of the Global Internet Liberty Campaign, the world's first international coalition of Non-Governmental Organizations concerned with the rights of internet users to privacy and free expression. He is a member of the Advisory Committee to the US Census and the Blue Ribbon Panel on Genetics of the National Conference of State Legislatures. He was a member of the US delegation to the recent G-8 Government and Private Sector Tokyo conference on Cyber Crime. Steinhardt has spoken and written widely on privacy and information technology issues.