International Campaign Against Mass Surveillance

THE EMERGENCE OF A GLOBAL INFRASTRUCTURE FOR MASS REGISTRATION AND SURVEILLANCE

International Campaign Against Mass Surveillance

THE EMERGENCE OF A GLOBAL INFRASTRUCTURE FOR MASS REGISTRATION AND SURVEILLANCE

Published April 2005

For more information, contact: info@i-cams.org

Table of Contents

International Campaign Against Mass Surveillance

THE EMERGENCE OF A GLOBAL INFRASTRUCTURE FOR MASS REGISTRATION AND SURVEILLANCE

"Eternal vigilance is the price of liberty."

- Wendell Phillips, 1852

THE ROAD WE ARE HEADING DOWN

On September 11, 2001 a number of persons supported by networks inside and outside of the United States executed one of the largest attacks ever made against civilians on American soil.

The Bush Administration responded quickly by propelling the *USA* PATRIOT ACT and other legislation through Congress that it said would fight terrorism, and by demanding that other countries follow the template provided by these pieces of legislation. Much of the Bush Administration's agenda was backed by U.N. Security Council Resolution 1373, under which member states failing to comply risked Security Council sanctions. But the agenda was also backed by the economic, political and military might of the United States. Under this pressure, and often for their own opportunistic reasons, many governments in the North and South, East and West have followed suit with a growing web of anti-terrorism laws and measures.

The result has been an emerging trend toward the harmonization and integration of security functions on a global scale. In democratic countries, this has led to a rollback of rights, freedoms, and civil liberties that have been won by centuries of popular struggle. In undemocratic countries, repressive regimes have been enabled and strengthened, and development assistance has been diverted to bolster security apparatuses. Internationally, the post-World War II order – which enshrines the universal, inalienable human rights of all individuals – has been seriously eroded.

Governments have been telling us that we must be willing to sacrifice some of our freedoms for greater security. Authorities say they need extraordinary powers to protect us from terrorists, and that we should be willing to put up with some inconvenience and invasion of privacy. Those who have nothing to hide, we are told, have nothing to fear.

But in this new world where individuals are expected to hide little from governments, governments are hiding a lot. And, there is a lot to be feared.

Myth #1 We are merely being asked to sacrifice some of our privacy and convenience for greater security.

Under the radar screen of the public, a global registration and surveillance infrastructure is quietly being constructed. It consists of numerous initiatives, most of which have been agreed to by governments without any democratic debate through international forums, treaties and arrangements. Many of these initiatives are now being implemented or are about to be implemented. Some are still in the research or proposal stage. Most of them require governments to override or ignore existing domestic and international legal obligations.

Although some of these initiatives have been reported in the press, it is difficult to grasp their significance by looking at each one in isolation, as they are often presented by the media. Viewed together, it can be seen that these initiatives aim to ensure that almost everyone on the planet is "registered", that all travel is tracked globally, that all electronic communications and transactions can be easily watched, and that all the information collected about individuals in public or private-sector databases is stored, linked, and made available to state agents.

Governments are not just collecting individuals' personal information and checking it against information about known terrorists, or those suspected of terrorism on "reasonable grounds". They are using it to assess "risk levels" for all of us, and sharing it with foreign agencies, with little or no control over how those agencies will use the information.

The object of the infrastructure that is being constructed is not ordinary police or intelligence work but, rather, mass surveillance of entire populations. In this infrastructure, everyone will be treated as a suspect, and state agents will maintain data profiles on all of us.

A major paradigm shift is occurring. Governments are no longer focussed on law enforcement and intelligence-gathering about specific risks. They have embarked on a much more ambitious and dangerous enterprise: the elimination of risk. In a "risk assessment" system, many of the ordinary legal protections that are fundamental to democratic societies – due process, the presumption of innocence, rights against unreasonable search and seizure and the interception of personal communications, and rights against arbitrary detention and punishment – go out the window. For the risk screeners, guilt or innocence is beside the point. What matters is the avoidance of risk from the point of view of the state, "separating the risky from the safe on the basis of the best information available from all sources…".[1] In this exercise, however, the "best information" need not be complete or even accurate: it need only be available.

In a risk avoidance model, the information appetite of states is infinitely expandable,[2] as they increasingly orient themselves to the future and concern themselves with the predictive power of the information gathered.[3]

There are, of course, historical antecedents of this kind of system – the witch hunts of the McCarthy era, the registration of the Jews in Nazi Germany, the secret files of the Stasi. But the system that is currently being constructed is unlike anything that has come before, for two reasons. First, its technological capacity dwarfs any previous system and makes Orwell's book *Nineteen Eighty-Four* look quaint. Second, its global reach ensures that one has to worry, not just about what one's own state might do with one's personal information, but about what any other state might do.

Indeed, it is now evident and documented that the United States and other countries are acting aggressively on information, seizing and detaining people without reasonable

grounds, and "rendering" them to third countries or extraterritorial camps run by the U.S., where they face torture during interrogation and indefinite detention. Alongside the global system for mass registration and surveillance is emerging what some commentators are calling a "global gulag",[4] in which unknown numbers of people are languishing. What is at stake in this new world order is more than mere privacy, or even democratic processes, legal systems, and civil liberties. Basic human rights are in jeopardy.

Governments promote mass surveillance initiatives as technical solutions to the problem of terrorism, and it may be that governments believe that these initiatives will do something to prevent terrorism. Certainly, governments believe that they must be seen to being doing something. But the questions we all should be asking our governments are these: *is* general and pervasive surveillance an *effective* response to terrorism? Is it proportionate to the real risk posed by terrorists? Will it destroy the very democratic societies it is supposed to be protecting and entrench the kind of corrupt, oppressive regimes that breed fanatical opposition and terrorism?

Are governments, in fact, also being opportunistic? Are they using the excuse of fighting terrorism to embrace initiatives that have consistently been defeated in democratic and legal processes, for purposes other than anti-terrorism, that is, in order to suppress dissent, enforce their hegemonic interests, keep out immigrants and refugees, increase ordinary law enforcement powers, and generally enhance the control they have over their populations?

What are the economic drivers in these initiatives? Are governments trading away their sovereignty and the real security of their citizens to appease the United States for economic reasons? Are there corporate interests in deep integration with the U.S.? Are there corporate interests in a global system of mass registration and surveillance?

Why are governments leading us headlong down this road?

What follows is an attempt to answer these important questions and to flag the "signposts" on the road governments are leading us down that show just how far down the road we have traveled and the dangers that lie ahead for all of us if we fail to make governments turn back. Ten of these signposts will be examined in detail. They can be summarized as follows:

• The *first signpost* was the effort of the United States to ethnically profile Muslim, or potentially Muslim, immigrants and visitors, and to register and/or detain them under immigration laws and programs called NSEERS and US-VISIT.

• The *second signpost* was the move on the part of the U.S. and its allies to do through international channels what most of them could not do through their own democratic systems – to expand registration to their own populations and create what is, in effect, a global identification system. This was accomplished by requesting the International Civil Aviation Organization (ICAO) to introduce a "biometric" passport that would be imposed universally.

• The *third signpost* was the creation, by similar means, of a global infrastructure for the surveillance of movement – using the biometric passport and airlines' passenger name records. Under this system, information about where individuals fly, and how often, will be tracked, stored, and shared between countries, and used to control the movement of people across borders.

• The *fourth signpost* was the creation of an infrastructure for the global surveillance of electronic communications and financial transactions. Through this infrastructure, state agents from our own and other countries will

have cost-free, direct access to individuals' e-mails, phone calls, and website browsing, and financial institutions will monitor transactions and report on them to state authorities.

• The *fifth signpost* is a development that feeds into all of the others – the radical convergence of government and private-sector databases, nationally and internationally. This is taking place under new laws, but businesses are also voluntarily surrendering databases to government agencies, and the U.S. government is purchasing databases, domestically and abroad. The result is the creation of a global web of databases that will be used by the U.S. and other countries (in conjunction with the infrastructures for the global surveillance of movement and of electronic and financial transactions) to generate detailed information dossiers on everyone.

• The *sixth signpost* is the growing number of mistakes and abuses that demonstrate the dangerous flaws inherent in the "risk assessment" paradigm that is driving the collection, storage and linkage of so much information.

• The *seventh signpost* is the deep integration of countries' police, security intelligence and military operations with American operations that governments around the world are acquiescing to, and their concomitant abandonment of national sovereignty and control.

• The *eighth signpost* is the huge profits being made by corporations in the new global mass registration and surveillance order, and the emergence of a new "corporate security complex".

• The *ninth signpost* is what is happening to democratic societies – in terms of the erosion of democratic processes , centuries-old protections in criminal law, freedom of speech and association, and the rule of law itself as governments pursue the agenda for global, mass registration and surveillance.

• The *tenth signpost*, and perhaps the most ominous of all, is the collective loss of moral compass societies are exhibiting as they begin to accept inhumane and extraordinary practices of social control. Countries that hold themselves out as defenders of human rights are engaging directly in extra-legal rendition, torture and extra-judicial killing – as well as contracting out these services to brutal regimes which are being rewarded for their contributions.

The attacks of September 11, 2001 in the United States and a subsequent attack in Madrid, Spain on March 11, 2004, made people everywhere realize that terrorism can happen in any country, and that technologically it has the potential to inflict harm on large numbers of people. The attacks were reportedly carried out by Muslims extremists who had gained legal entry to the country of their target, were technologically sophisticated, and had financial backing from sources inside and outside the country. These are facts that must be grappled with and addressed. However, the conclusion that must be drawn from a careful examination of the facts described in this report is that the initiatives that governments have embarked on *do not* create real security: they provide only the illusion of security. Steps that could be taken to effectively address terrorism – such as investing in on-the-ground human intelligence instead of technological surveillance, building bridges with Muslim communities, and helping to eradicate the poverty and oppression that are often the root causes of terrorism – are being given low priority by governments as they pursue their agenda of a global system for mass registration and surveillance. At the same time, the checks and balances that are essential to safeguarding person-

al liberty and security are being stripped away. The net result is that we are now less safe, not more.

It's time to tell our governments what we think – and to demand that they turn back from the dangerous road they are leading us down, before it's too late.

FIRST SIGNPOST: THE REGISTRATION OF POPULATIONS

In 1930s Germany, the Holocaust began with the simple registration of people of Jewish descent. First, they were registered, and then the state began an incremental stripping-away of their civil rights. In the countries invaded by the Nazis, the death rate of Jews was directly related to the census information available. In Norway, which had a population register, 50 percent of Jews were killed – compared with only 15 percent in Denmark and 0.5 percent in Finland.[5]

A full analogy does not need to be drawn to current circumstances to make the point that the registration of populations by ethnic origin, race, religion, political belief, or similar personal characteristics – while used for benign purposes in some countries – can also be a dangerous thing, easily abused by those in power.

One needs only to recall the internment of Japanese citizens that took place in North America during the 2nd World War, the 1994 genocide that took place in Rwanda,[6] and the Pass Laws of apartheid South Africa to know this is true. Registration is the tool by which those in power can easily single out and target certain kinds of people – not for what they have done, but for who they are.

1. Mass Detentions of Muslim Immigrants and Registration through NSEERS

One of the first actions of the U.S. government after September 11, 2001 was to ethnically profile and detain hundreds of Muslim non-citizens. These people were denied their legal rights to counsel, *habeas corpus*, speedy charges, and freedom from inhumane treatment and arbitrary detention.[7]

The U.S. government then went on to systematically register and create dossiers on nearly every male over the age of 16 with origins in a list of designated (mostly Muslim) countries, visiting the United States or traveling to or through the country.[8] This was done under a program called the National Security Entry-Exit Registration System (NSEERS). Many stories of harassment, insult, and rough treatment were told by the over 80,000 people[9] registered. Muslims and people with origins in Muslim countries felt unjustly targeted, and responded with outrage and fear.

NSEERS resulted in more than 13,000 people being put into deportation hearings.[10] Thousands more left the country in fear, decimating communities.[11]

2. US-VISIT and the E.U. Visa Information System

a) Biometric Visas

Under the recently inaugurated US-VISIT program, the registration that occurred through NSEERS is being expanded to most visitors to the U.S.[12] People applying for a visa for travel to the U.S. will now be registered by having their photographs and fingerprints taken at "virtual borders" outside the country, and citizens of visa waiver countries will be photographed and fingerprinted on entry. Photo and fingerprint data will be stored in a central U.S. database and inside a computer chip in each visitor's visa.[13] The technology being used to do this is known as "biometrics". It encodes the physical characteristics of a person – such as facial dimensions, fingerprints, iris patterns or voice patterns – into a computer chip or

database, so that the identity of the person carrying the chip can be verified against the information in the chip and/or database.

A similar program in the E.U. called the Visa Information System is being developed following a Decision of June 2004. It will capture and store all of the information, including biometric data, from visa applications to the 25 E.U. member states – about 15 million per year.[14]

b) Linkage of Biometric Information to a Global Web of Databases

The plan in the US-VISIT program, however, is not merely to verify that the person carrying a visa is who he says he is, or even to check his photographs and fingerprints against those of known terrorists or of persons suspected of terrorism on "reasonable grounds". (At best, say analysts, the U.S. may have a few dozen photographs of suspected terrorists; it has no database of their fingerprints or any other biometric identifier.[15])

The *plan* is to create information dossiers on all persons entering the United States, to store these dossiers for 100 years,[16] and to link individuals' biometric data to a web of databases, encompassing over 20 U.S. federal government databases as well as U.S. commercial databases.[17] Moreover, there is evidence that U.S. VISIT will eventually be linked to other programs – so that the web of databases dossiers are compiled from could be even wider, and have a *global reach*. A Federal Register Notice published by the Transportation Security Administration's (TSA) on August 1, 2003, for example, stated that the TSA anticipated linking the US VISIT program with a program discussed later in this report, CAPPS II, when both programs became "fully operational".[18] CAPPS II, was a a passenger screening system that envisioned linking a virtually unlimited number of public and private sector databases together. It has since been replaced by a slightly modified program, Secure Flight, but the aim of the program remains the same: linkage of as many databases as possible. And Secure Flight will be accessing the databases of large data aggregating companies, many of which buy information on citizens in countries outside of the U.S. (see p.)

Potentially, the data accessed by the U.S. under US-VISIT and other programs described in this report could include information about individuals' medical histories, social benefits, driving records, immigration status, passport applications, criminal records, security intelligence files, census responses, tax returns, employment histories, address histories, banking records, credit card purchases, medical prescriptions, air travel patterns, e-mails, e-mail correspondents, Internet use, on-line purchases and Internet music selections, cell phone calls, Internet phone calls, and library, bookstore and video selections.

Insiders are calling the database that is being built by the U.S. the "black box", as no one knows exactly what it will eventually contain,[19] only that it will be as comprehensive as possible.

Of course, some convergence of databases was taking place before September 11, 2001, but since that date there has been a radical acceleration of this trend (for a full description, see p). In the post 9/11 world, the public can no longer rely on the existence of "firewalls" between databases that to some extent protected privacy until recently. Where once, one could be relatively confident that no business or government agency could know everything about one, now, this is no longer true.

c) U.S. Acquisition of Domestic and Foreign Databases

One development that would shock many people is the aggressive acquisition by the U.S. government databases domestically and abroad since 2001.

Some of this access has been obtained under the *USA PATRIOT ACT*, which gives the Federal Bureau of Investigation (F.B.I.) a procedure to access any business records held by American-based companies and their subsidiaries, whether the data pertains to American residents or to residents of other countries.[20] These records could include the masses of personal information held by credit card companies, computer and Internet companies, bookstore and video companies, and others. It could include employment information about the people who work for these companies. And, as governments outside the U.S. contract out more of their services to U.S. companies and their subsidiaries, it could also include public-sector information on citizens in countries outside the U.S.

In Canada, for example, the federal government has entertained a bid to conduct the 2006 national census from a group of companies led by Lockheed Martin Canada (a unit of the U.S.-based Lockheed Martin Corporation).[21] The provincial government of British Columbia has contracted out the operation of its Medical Services Plan and Pharmacare to Maximus B.C., which is owned by the Canadian subsidiary of the U.S.-based company, Maximus.[22] A number of B.C. Hydro services (such as customer relationship management, human resources, financial procurement services and information technology) are handled by a Canadian subsidiary of Accenture, a Bermudian company with its main office in the U.S.[23] Under the *USA PATRIOT ACT*, the FBI need only ask for seizure of the business records of these companies in order to obtain them. The special court set up under the *Foreign Intelligence Surveillance Act* which hears its requests has never turned down a government request in more than 14,000 applications.[24] When seizure is granted, a gag order is placed on the business involved, preventing them from telling anyone about it.

Access to private-sector information has also been obtained by the U.S. under the *Enhanced Border Security and Visa Entry Reform Act of 2002.* Pursuant to this Act, the U.S. has demanded that all airlines travelling to or through the U.S. provide U.S. authorities with access to their passenger databases (see Third Signpost, p.).

In addition to statutory access, U.S. government agencies are *voluntarily* being given access to individuals' personal information by the private sector. Many U.S. companies, institutions, and organizations have shown themselves willing to simply hand over information about their customers and members when asked by the F.B.I. and other agencies. Some believe it is the patriotic thing to do; others may be afraid, or eager to please the government. Examples include the following.

• In 2001, 195 U.S. universities and colleges voluntarily turned over personal information about their students to government agencies – 172 of them did not wait for a subpoena.[25]

• In 2001, 64 percent of U.S. travel and transportation companies voluntarily turned over information about their customers and employees.[26]

• In 2002 the American Professional Association of Diving Instructors voluntarily gave the F.B.I. a disk with the personal information of about 2 million people.[27]

• Under a program called InfraGuard, more than 10,000 private companies in the U.S. voluntarily exchange information with the government,[28] checking out security alerts and monitoring the computer activity of customers and employees.[29]

• The airline JetBlue voluntarily gave the Transportation Security Administration over five million passenger itineraries, which

were then given to the Pentagon and combined with data profiles on each passenger obtained from Axciom, a large data aggregator company.[30]

• Northwest Airlines denied sharing passenger records with the government when the JetBlue story broke, but later it was discovered that it had voluntarily given millions of passenger records to the National Aeronautics and Space Administration (NASA).[31]

• In April 2004, American Airlines admitted to sharing 1.2 million records with the Transportation Security Administration and four research companies that were bidding for a government data mining contract.[32]

• In May 2004, the biggest airline companies in the U.S. – including American, United, and Northwest – admitted to voluntarily handing over millions of passenger records to the F.B.I. after the 9/11 attacks.[33]

All of the above incidents occurred without the consent of the individuals whose records were involved and, for the most part, in contravention of the privacy policies of the organizations providing the information.

Alarmingly, the U.S. government has also been *buying* personal data on Americans and the citizens of other countries from commercial data aggregators. Inside the U.S., companies like DoubleClick boast that their data includes information from over 1,500 companies, adding up to information on 90 million households and records of 4.4 billion transactions.[34] Outside the U.S., the company ChoicePoint Inc. has collected information on hundreds of millions of residents in Latin America, without their consent or knowledge, and sold them to U.S. government officials in three dozen agencies. In Mexico, ChoicePoint has bought the driving records of six million Mexico City residents and the country's entire voter registry and sold them to the U.S. government. In Colombia, ChoicePoint has bought the country's entire citizen ID database, including each resident's date and place of birth, passport and national ID number, parentage, and physical description. It has bought personal data from Venezuela, Costa Rica, Guatemala, Honduras, El Salvador, Nicaragua, [35] and Argentina as well. The company will not reveal who sells the information to it, but privacy experts say that government data is often sold clandestinely to companies like ChoicePoint by government employees.[36]

d) The Template for the Global System of Mass Registration and Surveillance

In many ways, an examination of the US-VISIT program and the data acquisition that the U.S. has embarked on reveal the template for the project of global, mass surveillance. Driven and designed largely by the U.S., the project's goal is to link individuals' biometric data with a web of databases, so that information dossiers can be compiled for each individual and they can be screened for "risk".

In this "brave new world",[37] the U.S. and other governments' goal is to compile information dossiers on as many people as possible and to create an information infrastructure that is not merely domestic in scope, but has a global reach.

SECOND SIGNPOST: THE CREATION OF A GLOBAL REGISTRATION SYSTEM

1. Biometric Passports

The global introduction of a biometric passport is one way to achieve nearly universal registration of everyone on the planet, so that individuals can be easily identified, surveilled and assessed for risk.

In recent years, many countries in Asia have started or intensified efforts to implement bio-

metric national ID cards, notably, India, China, Hong Kong, Bhutan, Malaysia, South Korea, Thailand, the Philippines, Indonesia, and Vietnam.[38] In the western hemisphere, Mexico is planning to introduce a national ID card, and Chile and Peru already have them. But in most democracies to date, the idea of a national identity card has been anathema – associated with police states, and politically unsellable because of the effect it would have on civil liberties. Although some democracies have national identification cards, in most of these systems, the kind of information linked to the card is limited, and access is restricted to domestic officials for specific purposes.[39]

An internationally-mandated biometric passport is a politically palatable way of imposing a *de facto* identity document on citizens in all countries, and of making the information linked to such a document globally available.

a) "Policy Laundering" – Referral to ICAO

Like many other global surveillance initiatives, biometric passports have been the subject of discussion among states for some time. The International Civil Aviation Organization (ICAO), the organization that governs international civil aviation, has been researching biometric passports since 1995, but national and regional laws protecting privacy and civil liberties were barriers to the adoption of most models for their deployment until recently. The U.S. led "war on terror" breathed new life into these efforts.

The *USA PATRIOT ACT,* passed in 2001, required the U.S. President to certify a biometric standard for identifying foreigners entering the U.S. within two years. The U.S. *Enhanced Border Security and Visa Entry Reform Act of 2002* required all countries wishing to retain their visa waiver status with the U.S. to implement the technology necessary to meet the standard by October 2004[40] and designated ICAO as the standard-setter. Handing the matter over to ICAO ensured that the organization would finally produce biometric passport specifications and that all countries, including the United Staes itself, would ultimately be obligated to adopt a biometric passport.

With the prospect of "international standards" being imposed on them by the U.S and ICAO to relieve them of political responsibility, governments likely felt more free to dispense with their earlier concerns about biometric passport. In May 2003, the G8 countries (Canada, the U.K., France, Japan, Italy, Russia, Germany and the U.S.) jumped on the biometric bandwagon, entering into an agreement to implement a biometric passport system.[41]

The loose standards that ICAO subsequently set for biometric passports are giving governments leeway to adopt just about any model of deployment they choose.

b) The Model: Carte Blanche

At its spring 2004 meeting in Cairo, ICAO adopted globally interoperable and machine-readable specifications for biometric passports with facial recognition as the mandatory biometric standard, and fingerprints and iris scans as optional additional standards.

The ICAO specifications only require countries to implement systems which can verify the identity of passport-holders against the biometric information stored in the computer chip in their passports, and which can check that information against the biometric information of other individuals (on a terrorist suspect list, for example).

Critically, however, ICAO has given states full discretion to use biometric passports for other purposes.[42] Under the ICAO standards, states will have free rein to create central databases of all travellers' biometric information, to store

information other than biometrics on chips, to use biometric passports as "keys" to multiple state and private databases, and to use biometric passports for purposes other than anti-terrorism. If the US-VISIT program for biometric visas is anything to go by, the U.S. will be storing biometric passport information and linking it with every available database around the world to create dossiers on all travellers. In Europe, there is already talk of creating a central database of travellers' fingerprints and other personal information, even though this would likely violate E.U. data protection laws.[43]

c) RFID Chips

The leeway states have to store, link, and use biometric passport data for purposes than anti-terrorism is not the only reason to be concerned about biometric passports. ICAO has also adopted a standard which requires biometric information to be stored in "contact-less integrated circuits", a technology similar to RFID chips.[44] RFID chips, or radio frequency identification chips, are tiny computer chips with miniature antennae that can be put into physical objects. When an RFID reader emits a signal, nearby RFID chips transmit their stored data to the reader. "Passive" chips do not contain batteries and can be read from a distance varying from 2.5 cm to six to nine metres. "Active" or self-powered chips can be read from a much greater distance.

Like RFID chips, contact-less chips allow for identification at a distance, though at the present time, the ICAO standard only calls for identification within 10 cm . Anyone with a reader could, secretly if they wished, read the chip through a wallet, pocket or backpack. So, not only will the customs officials of one's own country have access to the information in one's identity document, but retail companies, identity thieves, and the agents of other governments will have access too. Contact-less integrated chips are also capable of being "written into" and could hold anonymous "security clearance" types of information inserted by government agencies.

If we are required to carry identity documents at all times, which may be the case if biometric identity checkpoints are expanded from foreign air travel to domestic air travel and other forms of transportation (see p.), we will be extremely vulnerable to the surreptitious reading of our identities. In the future, government agents could use this kind of technology to sweep the identities of everyone at, say, a political meeting, protest march, or Islamic prayer service, or even to set up a network of automated readers on sidewalks and roads in order to track the locations of individuals.

d) Biometric Passports and the Democratic Deficit

The way in which biometric passports are being introduced around the world, is a prime example of how governments have been acting in stealth, outside democratic processes, to build a global surveillance infrastructure.

In Canada, a proposal for a biometric national ID card was floated in fall 2002 and soundly rejected in a Parliamentary committee[45] and the forum of public opinion by the fall of 2003.[46] The proposal was officially dropped. However, after government restructuring in 2004, the committee examining the idea was relieved of its duties before its final report could be released, and the deployment of a biometric passport (starting in 2005) was announced.[47] These developments came as a complete surprise to most of the institutions and organizations engaged in the earlier debate about a biometric identity document. They had not heard about Canada's agreement at the G8 summit to implement a biometric passport system and there had been no public debate before that undertaking had been made. When the plan was

announced, the government claimed it had no choice in the matter; that if Canadians wished to participate in global travel, they would have to go along with the measure.[48]

In the U.S., where it is unlikely that a national ID card would ever be accepted by the public, there was huge resistance to the idea of turning drivers' licenses into a kind of national ID card which would link numerous state and federal databases.Yet the federal government has mandated a biometric passport for Americans through international fora without many of them even being aware of it.[49]

In the U.K., there was hot debate over a proposal to introduce a national ID card. Under criticism, the idea was put on the shelf by the government in October 2003,[50] But, the U.K government had already agreed in May 2003 to develop a biometric passport system with other G8 countries.[51] Then, in December 2004 the E.U. announced that mandatory biometric passports would be introduced with facial scans required from 2006 and fingerprints required from 2007.

The U.K. government then introduced an *ID Cards* bill proposing the same biometric data be included in a new national identity card issued to everyone renewing their passport and to all immigrants and refugees. Under the bill, cards will become mandatory once three quarters of the population have them. A new national population database is being developed as well. The *ID Card Bill* was passed by House of Commons on February 10, 2005, with 224 votes in favour and 64 against. More MPs abstained than voted.[52] At the time of writing, it is being considered by the House of Lords.

e) Flawed Technology and Assumptions

By the time biometric passports are fully implemented, they could be carried by well over one billion people.[53]

While biometrics are being touted as the only way to ensure secure identity documents, biometric technology is known to be seriously flawed. Facial recognition, in particular, has a high rate of false negatives (where the technology fails to recognize individuals) and false positives (where the technology matches an individual to someone else, incorrectly). U.S. government tests have shown that even when the identity of a document holder is being compared only to the biometric information contained in the document (a "one to one" comparison as opposed to a "one to many" comparison) using recent photographs, there is a rate of five percent false negatives and one percent false positives. The reliability rates quickly deteriorate as photographs become dated, rising to 15 percent after only three years for the best systems tested.[54]

Fifteen percent of a billion people could mean 150,000,000 people misidentified! Even the people who invented biometric technology admit that it is dangerously flawed. George Tomko, regarded as one of the fathers of the technology, says that even a 99.99 percent accuracy rate – which doesn't exist for any of the identifiers – could leave millions of people vulnerable to mistaken identity.[55]

Moreover, determined terrorists could use false identities to obtain biometric identity documents. A security breach like the one suffered by the data aggregating company ChoicePoint recently – which allowed thieves access to personal data on 145,000 people – could help terrorists gain false documents.[56] Terrorists can also be successful using their own identities. All but two of the known 9/11 hijackers travelled in and out of the United States using their real identities.[57] Spain had a national identity card system at the time of the March 2004 Madrid bombing, but identity cards did not assist authorities in preventing the plot.

f) Expansion to Other Transportation Systems

Governments have recently been talking about expanding the security measures that are being implemented for air travel to other transportation systems.[58] If this happens, the use of biometric identity documents would expand exponentially, and transport systems could become the kind of internal checkpoints generally associated with police states.

g) Institutionalizing "Non-Personhood"

Of course, in a global identity system predicated on the avoidance of risk, not being registered or having a personal profile will amount to being a "non-person". By creating inclusion, the system also creates exclusion. For practical purposes, a person without a mandatory identity document will not exist – or will exist only as a risk to the state.

If one doesn't have an identity document (because it has been lost or stolen or withheld through a bureaucratic mistake) or a data profile (because one is poor, or a conscientious objector, or doesn't participate in the kinds of activities by which data is collected) – one will be, by definition, a risk. And one will be *at* risk, since the state will deal with one aggressively, according one few, if any, legal safeguards.

THIRD SIGNPOST : THE CREATION OF AN INFRASTRUCTURE FOR THE GLOBAL SURVEILLANCE OF MOVEMENT

The biometric passport and the biometric visa are components of a larger infrastructure that is being set up for the global surveillance of movement. This infrastructure includes another initiative: the sharing of passenger name record (PNR) information.

PNR information is the information kept in air travel reservation systems. It can include over 60 fields of information, including the name and address of the traveller, the address of the person with whom the traveller will stay, the trip itinerary, the date the ticket was purchased, credit card information, seat number, meal choices (which can reveal religious or ethnic affiliation), medical information, behavioural information, and linked frequent-flyer information.

1. U.S. Demands for Sharing Passenger Name Records

In its *Aviation and Transportation Security Act*, the U.S. required foreign air carriers to make PNR information available to its customs agency on request, and provided that this information could be shared with other agencies. The Bush Administration then passed an interim rule in June 2002, which interpreted the legislative requirement broadly. The rule required:

• that carriers give U.S. Customs *direct* access to their computer systems;

• that data be available for *all* flights, not just those destined for the U.S.;

• that once transferred, data be made available to federal agencies other than Customs for national security purposes or as authorized by law; and

• that the U.S. be permitted to store transferred data for *50 years*.[59]

Airlines, faced with fines and the possible denial of landing rights in the U.S., began giving the U.S. what it wanted, even though they were violating core principles of the privacy laws in their home countries. These principles require:

• restriction on the disclosure of personal information to third parties;

• limits on the use of data to the purpose for which it is collected;

• retention of data only as strictly required for a declared use;

• legal redress for individuals to correct inaccurate data or challenge misuse of data; and

• the maintenance of data security by the data holder.[60]

National governments in the countries where these air carriers were based were then left with the question of whether to enforce their privacy laws against the airlines or to allow the information transfers. At the same time, the U.S. government was approaching them to negotiate formal bilateral agreements for the sharing of PNR.

2. The Deals Made

In Canada, where the government was planning its own PNR system, and in December 2001, had agreed to share PNR information in some way with the U.S.,[61] an exemption to the Canadian data protection act was quietly pushed through Parliament. It allowed Canadian carriers to disclose any passenger information in their possession to a foreign state if required by the law of that foreign state.[62]

In Europe, the European Commission reached an agreement on PNR sharing with the U.S. in December 2003.[63] To do so, the Commission made a highly-contested ruling about the "adequacy" of U.S. undertakings to protect the privacy of European information in conformity with the E.U. *Data Protection Directive*.[64] In fact, the deal breaches many of the core principles in the *Directive*.[65] Data is being collected for multiple, undeclared purposes and will be shared widely among the numerous entities that make up the U.S. Department of Homeland Security.[66] Once stored in the U.S. there are no guarantees that information will not be shared or even transferred wholesale to third countries.[67] There is no clear right of access for individuals, no judicial right of redress,[68] and no requirement that the data be stored for the shortest possible time.[69] Tellingly, the deal left open the question of whether the personal data of European citizens would be used in the U.S. Computer Assisted Passenger Pre-Screening System ("CAPPS II"), even though it was known at the time of negotiations that the U.S. was *already* using European data to test the program.[70] (the aim of CAPPS II was to use PNR and other information to "risk score" all airline passengers. It has since been replaced with a program called Secure Flight – see p.).

3. PNR and the Democratic Deficit – Another Referral to ICAO

Usual democratic processes were circumvented in order to conclude the E.U.-U.S. arrangement. The deal was voted down three times by the European Parliament, the only directly elected body in the E.U., which referred the question of "adequacy" to the European Court of Justice.[71] Both the Parliament and the Court were overridden when the Council of the E.U. (the legislative body made up of representatives of the national governments in the E.U.) reverted to its treaty powers to rubber-stamp the deal.[72]

Some E.U. governing bodies, in fact, had their own ambitions to create a system for the collection and use of PNR data.[73] This plan was nodded through by the E.U. Justice and Home Affairs ministers in April 2004, just in time to avoid a new "co-decision" procedure that came into force on May 1, 2004, which would have required approval by the E.U. Parliament. National parliaments were also by-passed – the right of the U.K. Parliament to scrutinize the document was, for example, overridden by the U.K. government.[74]

Moreover, the E.U., to avoid further controversy, referred the matter of PNR sharing to ICAO, asking it to develop global standards.[75]

As with biometric passports, then, a global system will be established by an unelected, international body, and governments will be given an excuse for doing what their laws and citizens might otherwise have prevented. To date, only the U.S., E.U., Canada, and Australia have passed legislation to set up PNR sharing systems,[76] but others will surely follow once ICAO standards are adopted.

4. Expansion to Other Transportation Systems

As mentioned earlier (p.), government officials are talking about expanding the security measures that are being implemented for international air travel to other transportation systems. Canada, for example, indicated its intention to expand its PNR system to different modes of transportation in a submission made to ICAO in spring 2004,[77] and has already expanded the system to include domestic air travel.[78] The Department of Homeland Security has made similar suggestions with respect to the planned air passenger screening system in the U.S.[79] (see p.).

Myth #2: These initiatives facilitate travel.

The public relations spin about PNR sharing is that it will facilitate travel. "Now you can travel to Florida", we are told.[80] A more appropriate tag might be, "buy a ticket, get a record" – or "buy a ticket, take your chances".[81]

In the countries that currently have legislation permitting PNR data sharing, PNR data are being stored and used to create data profiles on individuals, so that these can be "data mined" using computer algorithms to "identify risk" (see p.). There are no legal avenues of redress to challenge one's risk "score". Those who are pulled over as moderate or "unknown" risks will miss flights. Those who are flagged as high risk may be "rendered" by the United States and other countries, without any kind of due process, to third countries where they may face torture, arbitrary detention, and even death (see p.).

FOURTH SIGNPOST: THE CREATION OF AN INFRASTRUCTURE FOR THE GLOBAL SURVEILLANCE OF ELECTRONIC COMMUNICATIONS AND FINANCIAL TRANSACTIONS

Along with the creation of a global registration and identification system and an infrastructure for the global surveillance of movement, governments are now working to substantially enlarge their powers to intercept and surveil electronic communications.

It is the historical tendency of law enforcement agencies, and governments concerned with law enforcement, to push for ever-greater surveillance powers. In democratic countries, civil liberties laws and traditions have acted as a brake to their overreaching, insisting that governments balance the law-enforcement interests of the state against the rights of the individual to be left alone and to be free from unreasonable search and seizure. However, these tenuous counterweights have been overridden in the period since September 2001 as many countries have adopted anti-terrorism legislation that has expanded state agents' interception and search and seizure powers and weakened or removed judicial oversight over those powers.[82]

But something else is happening, too. The private sector is being pressed into service as the state's eyes and ears. Just as it has done with the acquisition of private-sector databases and airline passenger record systems, the state is using the private sector to exponentially increase its surveillance capacity in the realm of electronic communications and financial transactions. And, instead of relying on the inconsistent practices of businesses, govern-

ments are starting to tell businesses how to design their information systems, what information to gather, how long it must be stored, what must be checked and reported, and what must be given directly to state officials.

1. "Building in" Surveillance[83] and the Convention on Cybercrime

Since 1994, land line telephone companies in the U.S. have been required by the *Communications Assistance for Law Enforcement Act* (*CALEA*) to *design* their equipment according to the F.B.I.'s specifications, in order to give law enforcement officials a "back door" through which they can wiretap the systems. In March 2004, the F.B.I., U.S. Department of Justice, and U.S. Drug Enforcement Administration asked for *CALEA* to be expanded to cover wireless service providers and any new communications technology coming on-stream. The F.B.I. and other law enforcement agencies have also pushed for an aggressive interpretation of *CALEA* that would allow monitoring of certain Internet content without a warrant, as well as the collection of information about the physical locations of cell phones.[84]

Of course, law enforcement and security intelligence officials in the U.S. always had access to these kinds of systems under interception and search and seizure warrants requiring service providers' cooperation. But, prior to *CALEA*, authorities' access to information was limited by technical barriers in the technologies used by the providers, and by authorities' budgets for installing interception equipment.

Compelling service providers to "build in" surveillance capacity to their systems means that within minutes of receiving a warrant from a court, real-time interception of a person's Internet or voice over Internet use can be implemented with just a few computer strokes, making a connection between the computerized listening stations of law enforcement and the service provider's system. At the same time, tools like the F.B.I.'s "Carnivore" software can be used to search masses of information within a system for key words.[85] The access to personal information that could be gained in this way is virtually limitless, since there will be few technical impediments and little cost to the state.

The U.S. is pressing other countries to follow its lead and implement more intrusive interception and search and seizure laws. Specifically, it is pushing for the global adoption of the Council of Europe's *Convention on Cybercrime*, which would toughen and harmonize all countries' cyber-security laws and allow countries to carry out investigations across borders.[86]

Negotiations for the *Convention* were difficult and prolonged, and were apparently sliding toward deadlock because of the barriers in countries' various domestic laws, when the events of September 2001 galvanized the parties to conclude the agreement. In November 2001, the U.S. and 29 other countries signed the document, and as of November 2004, there were 45 signatories.[87] The *Convention*'s purpose is not limited to anti-terrorism, but includes ordinary law enforcement as well.

In order to ratify the *Convention*, signatories must first implement the legislative changes necessary to comply with it. One obligation is to require "service providers" to provide law enforcement with real-time or direct access to the content data (e-mail messages, documents) and traffic data (information about when and to whom messages were sent, and web pages browsed) in their systems.[88] Gag orders on service providers whose systems have been accessed are another of the *Convention*'s requirements.[89] Mandatory preservation orders (orders directed at service providers requiring

them to preserve information in their systems) are another.[90] Alarmingly, another aspect of the *Convention* is the requirement, in some circumstances, to provide mutual assistance to co-signatories even where the activity to be investigated is considered a crime only in the requesting country.[91]

Governments of each of the signatory states are now drawing up legislation to implement these measures.

As with the ICAO guidelines for biometric passports, citizens would do well to carefully study the exact requirements of the *Convention on Cybercrime.* It appears that the *Convention* requires less draconian measures than governments claim it does. The *Convention* does not require service providers to *design* their systems to provide direct, real-time access, for example, as the U.S., Canada,[92] and the E.U.[93] are asking them to do, but only to provide such access "within existing capabilities".[94] The *Convention* does not require the use of powerful word searching software like the Carnivore (DCS 1000) system developed by the F.B.I., which can scan millions of e-mails a second. Nor does it require warrantless access, such as the FBI is seeking, and such as Colombia's new *Anti-terrorism Act* and China's "Golden Shield" project provide, and such as state agencies in Russia and the Ukraine have sought in the past. [95]

Similarly, the *Convention for Cybercrime* does not require mandatory routine storage of data by communication service providers, like the E.U. has embraced. A proposal for mandatory storage[96] was defeated in *Convention* negotiations because of national concerns about privacy laws.

2. Mandatory Data Retention

In a letter dated October 16, 2001, the Bush Administration made a number of demands to the E.U., asking for cooperation in its "war on terror".[97] One of these demands was for the E.U. to require mandatory, routine data retention by communication service providers. The demand was made despite the lack of data retention laws in the U.S. and the absence of data retention provisions in the *Convention on Cybercrime*.

Mandatory data retention requires the private sector to save and store data it would otherwise erase (when the data were no longer needed, or as required by privacy laws). As such, mandatory data retention exponentially expands the amount of information that can be tapped into by state authorities.

In 2002, the E.U. *Data Protection Directive* was amended to allow member states to pass domestic laws on mandatory data retention of traffic data for all communications. (Previously, data could only be stored for billing purposes.) By the end of 2003, 11 of the member states had set up, or planned to introduce, data retention regimes with retention periods ranging from one to five years. The second draft of a Framework Decision released in April 2004 which would bind all member states, provides for retention of traffic data for 12 to 24 months and for "lawful access" to the data by police for the purpose of "crime *prevention*" – creating a virtual license for police to go on "fishing expeditions" through Europeans' personal data.[98]

3. Expansion of ECHELON

Officials within individual nations may still, for the most part, have to secure judicial warrants in order to intercept and surveil the communications made available through "built in" surveillance and mandatory data retention. However, on the international stage, state agents will have access to this "new frontier" *with no judicial oversight*.

In 1948, the U.S., the U.K., Canada, Australia and New Zealand created a program under which they trawled the world's telephone communications – to spy on other countries and to share information on each others' citizens that could not be obtained by their own officials under domestic laws. Since the early 1980s, this program has been called ECHELON, and has been expanded to intercept e-mails, faxes, telexes, electronic transactions, and international telephone calls carried via satellites. The five agencies participating in ECHELON are the National Security Agency in the U.S., the Government Communications Headquarters in the U.K., the Defence Signals Directorate in Australia, the Communications Security Bureau in New Zealand, and the Canadian Security Establishment in Canada.

Under the ECHELON program, millions of messages and conversations are analyzed daily for key words and traffic patterns.[99] Each of the five centres supplies dictionaries to the other four of key words, phrases, people and places to "tag". The tagged intercepts are forwarded straight to the requesting country.[100] The quantity of communications available to be spied upon without judicial warrant under the ECHELON program will expand exponentially once communications around the world are stored for longer periods pursuant to mandatory retention laws, and may also increase when communications are made technologically available for tapping pursuant to the *Convention on Cybercrime* in the participating countries. And, while Echelon was previously used as an espionage tool, in the current political climate it is likely to be used more and more for law enforcement purposes. The number of countries participating in ECHELON may also expand.

4. Mandatory Information-Gathering and Reporting for Financial Transactions

U.N. Security Council Resolution 1373, passed shortly after September 11, 2001, required states, among other things, to:

> …prevent and suppress the financing of terrorism, as well as criminalize the willful provision or collection of funds for such acts …[and] …to prohibit their nationals or persons or entities in their territories from making funds, financial assets, economic resources, financial or other related services available to persons who commit or attempt to commit, facilitate or participate in the commission of terrorist acts.[101]

Under the Resolution, states must report on their implementation of these measures, and states failing to implement measures face Security Council sanctions.

The Resolution, and activism on the part of the U.S. and the international financial Institutions in promoting harmonized standards,[102] have led to new national laws around the world that enlist financial institutions and ordinary businesses into the surveillance infrastructure.[103] Many of these laws require banks and businesses to do more than simply "build" surveillance capacity "into" their information systems. They also require them to actively *gather* information about their customers that they would not otherwise gather, to *report* to government on certain kinds of transactions, and to *check* their customers against government watch lists.

In the U.S., for example, the *USA PATRIOT ACT* has dramatically expanded existing requirements for banks and credit unions to report deposits by customers, lowering the threshold to $10,000.[104] Now, "any person engaged in a trade or business" is required to file a "Suspicious Activity" report when he or she receives that amount or more in cash.[105] This means that every plumber, shop owner, general contractor, car salesman and real estate agent will be inducted into the financial transactions surveillance infrastructure.

Section 326 of the *USA PATRIOT ACT* requires financial companies to check customers against government watch lists. Executive Order No. 13224, issued September 24, 2001, requires businesses involved in helping individuals buy or sell various kinds of property (such as pawn brokers, real estate companies and jewellers) also to check customers against government watch lists.

Regulations stemming from s. 314 of the *USA PATRIOT ACT* require financial institutions to search through their records for any transactions made by individuals suspected of money laundering by any arm of the U.S. government with a law enforcement function. Money laundering is a broad offense encompassing any attempt to disguise illicit profits in pursuit of more than 200 different crimes. In other words, under *USA PATRIOT ACT* regulations, agencies like the U.S. Agriculture Department and the Postal Service have the power to conduct a cross-country search for financial records matching someone they suspect of illicit dealings, whether these dealings are related to terrorism or not.[106]

Around the world, charities are also having obligations imposed on them in the bid to cut off funds for "terrorist" groups. In Canada, for example, the *Anti-Terrorism Act* imposes significant liability on charities accused of having links with terrorist organizations, including the de-registration of their charitable status and the seizure of their assets. Laws like these are having an enormous effect on humanitarian organizations operating in the conflict zones of the world, where it is often impossible to avoid direct or indirect contact with entities that are rightly or wrongly labelled as "terrorist".[107]

FIFTH SIGNPOST: THE CONVERGENCE OF NATIONAL AND INTERNATIONAL DATABASES

1. Radical Acceleration of Convergence Since 9/11

The collection of new information has been accompanied by a new and rapid convergence of information – a bringing together, or sharing of multiple sources of information so that larger and larger pools of information are accessible to state officials. Certainly, convergence has been a trend in the last couple of decades, a notable example being the Schengen Information System ("SIS") in Europe, which was set-up to compensate for the abolition of internal border controls and provided for the sharing of criminal and immigration information between certain countries.[108]

But there has been a radical acceleration of convergence, or sharing, of information since September 2001. U.N. Security Council Resolution 1373 (see pp.) calls on states to intensify and accelerate the exchange of information regarding terrorist actions and movements, and governments have been taking steps nationally and internationally to heed the call.

Some of the convergence that has been taking place since 9/11 has already been described:

• the convergence of private and public databases under the US-VISIT program;

• the access to domestic and foreign databases the U.S. has gained through purchase from "for profit" data aggregators;

• the voluntary sharing of data by the private sector in the U.S. at the request of U.S. government agencies;

• the access the F.B.I. has gained under the *USA PATRIOT ACT* to the business records of U.S.-based companies operating at home and in other countries;

• the creation in the U.S., the E.U., Canada, and Australia of central databases for PNR data;

• plans for the creation of a European-wide fingerprint register piggybacking on the biometric passport initiative;

• expanded access to information internationally under ECHELON; and

• private-sector reporting of financial transactions to government.

Many more examples of convergence could be added to the list:

• In Europe, in the name of combating terrorism, a second generation Schengen Information System, called SIS II, is being developed. It will cover 27 European countries, will share a technical platform with the E.U. Visa Information System (see p. ?? above) and will exist alongside the E.U. population database being developed as part of the biometric passport proposals (see p. ?// above).

• Under a U.S. program called "Multi-State Anti-Terrorism Information Exchange" or MATRIX, government data bases[109] from participating American states are being combined with a private database that claims to have "20+ million records from hundreds of sources".[110]

• In Canada, a Public Safety Information Network is currently under construction that will link together key justice records and possibly criminal investigation information, passport information, and travel information. It will be accessible to numerous Canadian agencies that formerly did not routinely share information, and will be interoperable with systems in the U.S. and other countries.[111]

• In Colombia, the new *Anti-terrorism Act* envisions the creation of a new registry containing private information on all Colombians, to which military authorities will have access.

• In Europe, an interim agreement signed between Europol and the United States, concluded without democratic oversight and without publication, will give an unlimited number of U.S. agencies access to Europol information – including sensitive information on the race, political opinions, religious beliefs, health and sexual lives of individuals. The agreement contravenes the *Europol Convention* and the E.U. *Data Protection Directive,* in that individuals cannot access their data if the U.S. does not agree, or request the correction or deletion of data.[112]

• The new E.U.-U.S. agreement on mutual assistance provides for cooperation in a number of areas including the exchange of banking information and for purpose . not limited to terrorism.[113]

• Joint investigation teams being set up between the U.S. and Europe under the agreement mentioned above, and between the U.S. and Canada,[114] could include customs, police, and immigration agents, as well as agents from organizations like MI5, the Canadian Security Intelligence Service (CSIS), the F.B.I., and the Central Intelligence Agency (C.I.A.). These teams will share information without the formal state-to-state requests required under mutual assistance agreements. Members of the teams will also be able to directly request their counterparts to facilitate interceptions, searches and seizures, arrests, and detentions, and may not be legally accountable for their actions on foreign soil.

• Existing mutual assistance agreements are being used in new ways. In October 2004, two computer servers were seized by the F.B.I. from the England office of the Texas-based internet company, Rackspace. The servers were hosting the website of Independent Media Centres. The seizure was reportedly made under a U.K.-U.S. Mutual Assistance treaty of

1996, but on the request of Swiss or Italian police.[115]

• In countries known for their oppressive regimes, the extent to which an integration of functions and information-sharing with the U.S. has been occurring is probably the greatest As discussed later in this report, countries like Georgia, Indonesia, Egypt, Malaysia, and Uzbekistan are sharing information, suspects, and in some cases, intelligence and military operations with the U.S. in the "war on terror"

2. The "Black Box" of Information

The "black box" of information that was described in the context of the US-VISIT program (p.) – the database of databases that the U.S. is currently amassing with the help of the convergences described above – could contain all of the information described above and more. Without doubt, it will be a global web of databases, encompassing domestic and foreign and public and private sector sources.

SIXTH SIGNPOST: THE DANGERS OF A RISK ASSESSMENT MODEL – A WORLD THAT IS BOTH ORWELLIAN AND KAFKAESQUE

But is there anything to fear if one is innocent?

1. Data Mining – The High-Tech "Solution" to Risk Assessment

A veritable ocean of information is being collected, stored, linked together, and shared. No country has the capacity to analyze it using human intelligence. The "high-tech" solution to this, which some governments are pursuing with fervor, is data mining.

a) Orwell Revisited

Data mining is the use of computer models, or algorithms, to scrutinize masses of data for selected criteria. In the "war on terror" world, data mining is being used to identify patterns of behaviour that are supposedly indicative of terrorist activity, in order to assess the level of risk that individuals pose to the state.

In Orwell's famous book, *Nineteen Eighty-Four,* the hero says:

> It was inconceivable that they watched everybody all the time. But at any rate, they could plug in your wire whenever they wanted to. You had to live – did live from the habit that became instinct – in the assumption that every sound you made was overheard.[116]

Orwell's book presents us with an imaginative, dark vision of what living in a surveillance society could be like, but the methods it describes are quaint in that they require human beings to watch others using auditory or visual devices. In the Orwellian society of the 21st century, we will be watched and assessed by computers. And the assessment will be based, not on our actual observed involvement in terrorist activity, but on the probability that we might be engaged in such activity.

Myth #3: If one has nothing to hide, one has nothing to worry about.

In the Cold War/McCarthy period in the United States of the 1950s, the maxim was that if any doubt existed as to the reliability or loyalty of an individual, such doubts should be resolved in favor of the state. As a historian of the period has said,

> Anyway, there was little or no interest in individuals, as such. Individuals were messy, unfathomable in their

> complexity and idiosyncrasy to bureaucrats who had to deal with large numbers of cases and in universal categories. Dossiers were neat, simple and serviceable for the specific purposes required ... Of course, it was possible that mistakes could be made, that information might prove faulty in some particulars, that innocence might be mistaken for something else…[117]

An example of the many mistakes that were made in that era was the naming of academic Owen Lattimore as the Soviet Union's top spy in the U.S. He later was fully cleared of the charges. In his account of the affair he noted that the F.B.I. and other agencies had "built up on him a dossier of 'a man who might have existed'".[118] Again, as a historian of the period has observed, "that phrase catches the very essence of the creation of the national insecurity state: a data world that shadows, mimics, and caricatures the real world".[119]

We may think that anyone looking at our personal data with the proper explanation would conclude we are innocuous, but, in fact, in the data world we have no control over our "virtual identities" or the interpretations that others make of them.

a) TIA, MATRIX and Other Data Mining Projects in Implementation or Development

The forerunner of all post-9/11 data mining projects was a program known as Total Information Awareness (TIA), run by Iran-Contragate's John Poindexter out of the Defense Advanced Research Projects Agency (DARPA). The goal of the program, as described by Poindexter, was to mine "the transaction space" to find "signatures" of terrorist activity. According to the program's website, the transactions mined would include individuals' financial, medical, travel, "place/event entry", transportation, education, housing, and communications transactions. Poindexter envisioned his program developing software that could quickly analyze "multiple petabytes" of data. (The 18 million books in the Library of Congress could fit into one petabyte 50 times over; one petabyte could hold 40 pages of information on each of the 6.2 + billion persons on earth.)[120] As the manager of the project described it, the task was:

> "…much harder than simply finding needles in a haystack. Our task is akin to finding dangerous groups of needles hidden in stacks of needle pieces. We must track all the needles all of the time."[121]

One of the researchers for the TIA project, David D. Jensen at the University of Massachusetts, acknowledged that the program could generate "high numbers of false positives …".[122]

Because the concept of "total information awareness" on the part of government bothered Americans so much, the program's name was later changed to Terrorism Information Awareness. Nevertheless, Congress pulled the funding from it in fall 2003.

TIA lives on, however, in hidden research projects and other programs. As Steve Aftergood of the American Federation of Scientists, which tracks work by U.S. intelligence agencies, has written:

> "the whole congressional action looks like a shell game. There may be enough of a difference for them to claim TIA was terminated while for all practical purposes the identical work is continuing."[123]

Congress has transferred some TIA funding to the National Foreign Intelligence Program which, it says, can only use its research against persons

overseas or against non-Americans within the U.S. But there is nothing to stop the government from expanding this program to American citizens at a later date or through other programs. Some say parts of the original TIA program live on in the Pentagon's secret "black budget".[124] People with direct knowledge have told the press that the surviving TIA programs include some of the 18 data mining projects collectively known as Evidence Extraction and Link Discovery.[125]

In its May 2004 report on federal data mining efforts,[126] the U.S. General Accounting Office (now known as the Government Accountability Office, or GAO) revealed at least four projects that use personal information from the private sector. One of these, run by the Defense Intelligence Agency, mines data "to identify foreign terrorists or U.S. citizens connected to foreign terrorism activities". The National Security Agency has a program called Novel Intelligence from Massive Data, which is supposed to extract information from databases including text, audio, video, graphs, images, maps, equations, and chemical formulae. The C.I.A. reportedly has a data mining program called "Quantum Leap" which "enables an analyst to get quick access to all the information available – classified and unclassified – about virtually anyone". The deputy chief information officer of the C.I.A. told a reporter that the program's technology "is so powerful it's scary".[127]

MATRIX (see p. above). is another data mining initiative of the U.S. government. Information on the false positive rates for this programs is not readily available. But an indication of the rate can be gleaned from the number of people Seisint Inc. told state authorities showed statistical likelihood of being terrorists in its bid for the contract to develop MATRIX: 120,000.

b) CAPPS II

The data mining program to which U.S. VISIT was supposed to be linked (see p.), CAPPS II, or the second-generation Computer Assisted Passenger Prescreening System, was designed to use algorithms to sort through PNR (see p.) and other information in order to "risk score" all airline passengers as "green", "amber" or "red". "Green" stood for minimal risk, "amber" for an unknown or intermediate risk requiring heightened security measures, and "red" for high risk, requiring grounding of the passenger and reference to law enforcement for detention. The criteria for assigning the scores were undisclosed.

According to a notice published in the U.S. Federal Register in January 2003, the intent of the Transportation Security Administration (TSA), the agency developing CAPPS II, was to create a screening database that would be linked to virtually unlimited amounts of data from private and public sources, including "financial and transactional data". Also, numerous public and private entities were to have access to the system.[128]

The TSA estimated that five percent of the travelling public would be rated "amber" or "red" under the CAPPS II program.[129] The program contained no mechanism by which a passenger could challenge her score. The Association of Corporate Travel Executives estimated in a study that if only two percent of travellers were rated "red", there would be up to eight million passengers detained or denied boarding every year under CAPPS II.[130]

The GAO issued a report in February 2004,[131] in which it said the TSA had failed to show that CAPPS II was effective in identifying possible terrorists and had failed to resolve crucial privacy issues of oversight and passenger redress.

In July 2004, there was news that the government had bowed to pressure from the GAO, civil libertarians, and airlines and decided to kill the CAPPS II program.[132] However, it soon became clear that the program was only being modified

and postponed.[133] A Homeland Security spokesperson said that a new screening program would rise from the ashes of CAPPS II and that it would cover all passengers travelling to, through, or within the country.[134] In August 2004, a new passenger-screening program called "Secure Flight" was announced.[135]

The Secure Flight program will not be looking, as CAPPS II was designed to do, for people with outstanding warrants in respect of ordinary criminal offenses – a proposal criticized by many as an expansion of law enforcement powers that was unnecessary for airline safety. But, like CAPPS II, it will consult commercial databases, such as those owned by data aggregators Acxiom and Lexis Nexis to verify passengers' identities. The government claims that Secure Flight will not incorporate CAPPS II-style computer algorithms for "risk scoring" passengers.[136] However, one wonders whether this feature may be reintroduced in the future, especially as the government's data mining research becomes more advanced.

c) Canadian Risk Assessment Centre

Since January 2004, Canada has been engaged in setting up a data mining, risk scoring program to complement the American CAPPS II/ Secure Flight program.

Few details are publicly available about how it will operate, except that it will be interoperable with the U.S. program and that it will use computer screening. The criteria for identifying high-risk travellers are undisclosed but the program will probably rely on the same criteria used by the American program. The information used will include PNR data on air passengers on incoming, outgoing and domestic flights.[137] The federal government intends to eventually expand the program to border-crossing passengers using all modes of transportation.[138]

d) German "Trawling"

After September, 2001, German police units started collecting data on young men with Islamic backgrounds from universities, registration offices, health insurance companies and Germany's "Central Foreigners Register" (*Ausländerzentralregiste*) using the practice of "trawling" or "dragnet control" (*Rasterfahndung*). Introduced in the 1970s in the wake of the activities of the terrorist group *Rote Armee Fraktion,* it allows *v*ast amounts of data to be collected about individuals and compared to various criteria.

The "profile" used in the program after 9/11was that of the Arab students from the University of Hamburg allegedly linked to the 2001 attacks in the U.S. – effectively making every male Arab student in Germany a suspected terrorist. As a result of the program, approximately 10,000 students have been placed under surveillance in North-Rhine Westphalia (NRW) alone.[139]

e) Data Mining and the Democratic Deficit

As with other mass surveillance initiatives, there has been a democratic deficit in the implementation of data mining programs.

First, there has been a conspicuous lack of transparency about these programs. It is difficult to get information about what projects are being undertaken and how they will operate. Many, like the Canadian initiative, have been set up quietly, under the radar of the public, with little or no democratic debate.

Accountability for data mining programs is avoided by governments. For example, the implementation of the highly criticized CAPPS II/ Secure Flight program was postponed until after the American election in November 2004, and government officials would not give details about what they were keeping or drop-

ping in the program before the election.[140] Finally, governments are less than honest about these projects. The TSA, for example, told the press, the GAO, and Congress that it had not used any real-world data in the testing of CAPPS II. This later turned out to be patently untrue[141] When programs are cancelled under democratic pressure, governments simply re-introduce them in new packages.

f) Flawed Facts, Dirty Information, "Guilt by Google", Ethnic Profiling

The post-9/11, data mining version of the McCarthy era is, perhaps, a bit like the Hollywood film *Minority Report* – in which state officials try to use technology to read people's minds in order to stop criminal acts before they happen. However, the technology that is being used in the post-9/11 world falls far short of the technology of Hollywood fantasy.

Myth# 4: The technology being used is objective and reliable.

First, the factual base on which the technology rests is unreliable. The "best information available" on which data mining or risk-scoring technology depend is often inaccurate, lacking context, dated, or incomplete. It might even be dirty information – extracted by torture, or offered by an informant who is vulnerable or is acting in bad faith.

None of the data mining programs contains a mechanism by which individuals can correct, contextualize or object to the information that is being used against them, or even know what it is. Indeed, these systems are uninterested in this kind of precision. They would be bogged down if they were held to the ordinary standards of access, accuracy, and accountability. Operating on a precautionary principle, they are not really concerned with the truth about individuals: they are *meant* to cut a broad swath.

Secondly, the criteria used to sort masses of data will always be over-inclusive and mechanical. Data mining is like assessing "guilt by Google" key-word search. And since these systems use broad markers for predicting terrorism, ethnic and religious profiling are endemic to them. The manager of the TIA program was right when he said that looking for anything useful with data mining was like looking for particular needles in stacks of needles. However, his analogy would have been more accurate if he had talked about looking for a needle in an ocean full of needles.

2. Low-Tech "Solutions" to Risk Assessment

Of course, not all risk assessment in the "war on terror" is being done by computer data mining. As in the McCarthy era, human beings are also making judgments about who might present a "risk".

In the post-9/11 climate, where law enforcement and security intelligence agencies are being blamed for failing to stop the attacks on U.S. soil, there are strong bureaucratic incentives for officials to err on the side of caution. **After all, who would want to be responsible for failing to receive, gather, share, or flag information regarding someone who later turned out to be a terrorist? As with data mining, a precautionary principle is at work when human beings are making the risk assessments.**

This kind of environment leads to indiscriminate interpretations of information and indiscriminate actions on the part of authorities. And, as with high tech risk assessment, ethnic and religious profiling is endemic.[142]

a) Guilt by Association and Indiscriminate Sharing of Information: The Story of Maher Arar

On September 26, 2002, while returning from a family vacation in Tunisia, Maher Arar disap-

peared. A Canadian who had migrated with his family from Syria at the age of 17, Arar was a telecommunications engineer, a husband, and a father of two young children, and a Muslim.

It was not until six days later that Arar was able to call his mother-in-law in Ottawa to tell her that he had been taken aside at JFK airport in New York for interrogation and then transferred to a detention center. A consular official visited him October 3 and he was able to see a lawyer on October 5. Three days later, in the middle of the night, however, he was put on an airplane with U.S. agents and taken against his will to Jordan, and from there to Syria.

During his interrogation in New York, agents had questioned him about information they could only have received from Canadian sources. They wanted to know about Abdullah Almalki, the brother of a man he worked with, with whom Arar had a casual acquaintance. They produced a copy of Arar's Ottawa rental agreement, which had been signed by Abdullah Amalki. Arar told them he had asked Abdullah's brother to come over and witness the lease, but the brother had unavailable and had sent Abdullah. The American agents swore and yelled at Arar. His requests for a lawyer were refused and he was pressured to agree to be deported to Syria. He did not agree. He told them his mother's cousin had been accused of being a member of the Muslim Brotherhood and had spent nine years in Syrian prisons; he told them he would be tortured if they sent him to Syria.

Maher Arar was sent to Syria where he languished in a Syrian prison for almost a year, and was tortured. He heard the screams of other prisoners being tortured. His cell was the size of a grave – without lighting, hardly wider than his torso, and only two inches longer than his height. He thought he would die there.[143] However, the Syrians eventually released Arar on the basis that they had no evidence to continue to hold him. Syrian officials later said they had had no interest in Arar, and had only interrogated him in a show of goodwill to the United States.[144]

In Canada, the Arar affair became a cause célèbre. Canadians were shocked that a citizen with a Canadian passport could be sent to a third country for arbitrary detention and torture. They pressured the government to hold a public inquiry, which started its work in June 2004. All of the evidence has yet to come out, but it appears that Arar's name was passed on to U.S.officials by Canadian security officials who had noted him because of a casual encounter he had had with Abdullah Almalki, their primary target. Arar, it seems, had the misfortune to be observed eating with Almalki in a fast food restaurant, then talking on the street with him in the rain outside the restaurant.[145] This was enough to land him on a U.S. terrorist list.

Canadian authorities seem to have drawn conclusions of guilt about Arar from the most tenuous evidence of association. They did not have reasonable grounds to suspect him of anything when they passed his name on to a foreign agency. Either they had no regard for what might happen to him as a result, or they were in some way complicit in what subsequently occurred. How safe would any of us be, if we could be targeted on the basis of any association we had made in the many aspects of our lives? In relatively small religious or ethnic communities where most people know each other or have some shared acquaintances, hardly anyone would be safe.

Britain's most senior judge, Lord Chief Justice Woolf, upholding the release of a Libyan man who had been held without charges on secret evidence for 15 months under the U.K. *Anti-Terrorism, Crime and Security Act*, asked government lawyers:

> "If I was a grocer and I delivered groceries to somebody who was a member of al-Qaida, do I fall within that [the *Act's* definition of a terrorist]?"[146]

U.N. Security Council Resolution 1373 (see pps. [Intro and financial transactions]) called on all states to "take steps to prevent the commission of terrorist acts, including the provision of early warning to other states by exchange of information". The *Smart Border Declaration* and accompanying *Action Plan for Creating a Secure and Smart Border* negotiated between Canada and the U.S. after September 11, 2001 call for the sharing of information and intelligence in a timely way[147] and for joint intelligence teams.[148]

Certainly, the timely sharing of information among agencies and countries is an important part of combatting terrorist acts and other crimes. However, there need to be appropriate criteria about the quality of the information that can be passed on to foreign countries, and instructions or conditions about how the information can be used. In the Arar case, Inquiry testimony to date has revealed that neither of these safeguards was in place in Canada. Officials testified that many arrangements for sharing information with foreign agencies are merely oral, and that front-line officers have wide discretion about what they share and in what circumstances.[149]

As mentioned earlier, under the recent agreement between Europol and the U.S. (see p.), an apparently unlimited range of agencies in the U.S. will have access to personal data provided by Europol, and there is no condition prohibiting Europol data from being passed on by the U.S. to other countries.

b) Using Information Obtained by Torture and Tipping Off Torturers

Another example of indiscriminate behaviour on the part of authorities carrying out "low-tech" risk assessment is their use of torture.

Repressive regimes are not the only ones using torture to make risk assessments. Testimony from the Arar Inquiry has revealed that Canadian agencies may, in some circumstances, share information with foreign agencies they suspect are engaged in torture, and that they will receive and use information from foreign agencies obtained through torture if it is corroborated by other sources.[150] This is done even though Canada is a signatory to the U.N. *Convention against Torture*.

Reportedly, Canadian authorities may also wait for people to go abroad in order to have them questioned without a lawyer present and intimidated or mistreated by foreign security forces. In September 2004, the brother-in-law of Maher Arar, who had just moved back to Tunisia, was questioned by Tunisian secret police. According to Arar's family, the Tunisian questioners had information to which only Canadian authorities would have had access. Canadian authorities had had ample opportunity to interview the brother-in-law while he was living in Canada for four years, but had not done so.[151] Another man, Kassim Mohamed, who divides his time between Toronto and Egypt, was questioned by CSIS in Canada after videotaping Toronto landmarks for his children, who attend school in Egypt. He was then cleared to go to Egypt. When he arrived in Egypt, he was arrested and held for two weeks, handcuffed and blindfolded, in a prison in Cairo.[152]

In the U.K., the intelligence service MI5 appears to have tipped off the C.I.A. so that a British citizen of Iraqi origin, Wahab al-Rawi, could be seized by the C.I.A. when he arrived in Gambia for a business trip on a flight from London, and thereby deprived of his rights under British law. Al-Rawi has said that when

he asked to see British consul, the C.I.A. agent interrogating him laughed, saying, "Why do you think you're here? It's your government that tipped us off in the first place".[153]

The English Court of Appeal ruled in August 2004 that the use of evidence obtained under torture was legal in the U.K., as long as the U.K. neither "procured nor connived at" torture.[154]

(For an indepth discussion about the use of torture by the U.S. and other countries, see Tenth Signpost , p.)

c) Sloppy Mistakes: The Madrid Investigation

In the low-tech version of risk assessment, many "false positives" are the result of sloppy police work and crude profiling on the part of authorities.

The home of Brandon Mayfield, an American citizen and lawyer in Oregon, was secretly searched and he was thrown in jail for two weeks when the F.B.I. matched his fingerprint to a print found on a plastic bag used by terrorists in the Madrid train bombing of March 2004. The print was of poor quality and the Spanish authorities who had provided it warned American investigators early in the case that the print did not match Mr. Mayfield's.[155] But the U.S. Justice Department used a "material witness" law to round up Mr. Mayfield anyway on the evidence, bolstering their case by painting him as a Muslim extremist. The affidavit that secured the arrest made much of the fact that he had converted to Islam, was married to an Egyptian-born woman, and had once briefly represented one of the "Portland Seven" in a child custody case.[156]

Spanish authorities eventually matched the fingerprint, along with other evidence, to Ouhnane Daoud, an Algerian living in Spain.[157] Brandon Mayfield had not travelled outside the United States for over a decade.[158] The F.B.I., which originally said it was absolutely certain the print was Mayfield's, subsequently claimed it was "of no value for identification purposes".[159]

d) Getting People off the Street: Arbitrary Detentions

In the low-tech version of risk assessment, governments wanting to eliminate risk have indiscriminately swept people off the streets – using detentions without charge and indefinite confinements that violate constitutional guarantees and human rights obligations.

Under human rights law, arbitrary detentions are justified only in a time of public emergency which threatens the life of the nation, and only if the state publicly declares such an emergency. Then, the derogation from rights may only be carried out "to the extent strictly required by the exigencies of the situation", and without discrimination.[160]

As described earlier, the Bush Administration detained masses of people after September 11, 2001(see p.), and it did so without declaring the state of emergency required under international human rights law. The Administration had sought power to detain non-citizens without charge and without judicial review in the *USA PATRIOT ACT*, but Congress had refused this request. Undeterred, the Administration created the power on its own, by quietly issuing an administrative order. The order allowed INS to hold non-citizens on immigration charges for 48 hours without charges, and to extend that time indefinitely "in the event of an emergency or other extraordinary circumstances".[161]

The move was an end-run around democratic processes and around the constitutional protections for accused people in criminal processes. In criminal cases, the U.S. Constitution requires charges to be laid in a timely manner,

and guarantees detainees the right of *habeas corpus*.[162] The U.S. Supreme Court has held that the government must charge a detainee, and a judge must determine there is probable cause to substantiate the charge, within 48 hours.[163] By holding people on immigration charges while they were in fact being investigated for links to criminal activity (terrorism), the government deliberately sought to deny them these constitutional rights.[164]

During this period, some 1,500 to 2,000 people with origins in Muslim countries were rounded up and held,[165] and at least 762 were then charged with immigration charges and detained longer.[166]. The government refused to release the names of those held or to allow nongovernmental organizations to monitor their treatment. The average detention lasted for three months – until the F.B.I. determined that the individual had no links to, or knowledge of, terrorism.[167] None of those held on immigration charges has been charged with involvement in the September 11 attacks. With the exception of four people indicted in August 2002 on charges of support for terrorism, none had been charged with terrorism offenses as of September 2002.[168]

A 2003 report by the U.S. Office of the Inspector General confirmed that the government held many of these detainees on immigration charges for prolonged periods without charges, denied them *habeas corpus*, denied them contact with the outside world, impeded their right to counsel, overrode judicial orders to release them on bond, subjected them to coercive interrogations and solitary confinement, and allowed them to be physically and verbally abused because of their national origins.[169]

The U.S. has also been "getting people off the street" within its own borders by abusing "material witness" laws that allow police to hold someone for questioning without having probable grounds to hold them as criminal suspects (as in the Brandon Mayfield case described earlier). A district court judge has declared, "The government's treatment of material witness information is deeply troubling … The public has no idea whether there are 40, 400, or possibly more people in detention on material witness warrants"[170] The U.S. government is also holding U.S. citizens it has designated as "enemy combatants" – a term that does not exist in international humanitarian law. While the U.S. Supreme Court upheld detention on this basis in the case of Yaser Esam Hamdi, a U.S. citizen allegedly captured during hostilities in Afghanistan,[171] the U.S. District Court has recently ruled (on remand from the U.S. Supreme Court) against the government in the case of Jose Padilla, a U.S. citizen apprehended in the U.S.[172]

In the U.K., the government held more than a dozen foreigners in indefinite detention without charge under the *Anti-Terrorism, Crime and Security Act 2001*. As of October 2004, seven had been detained for more than two years. None had been charged with a crime. Indefinite detention was condemned by two U.K. parliamentary committees, both of which asked that the practice be "replaced as a matter of urgency", arguing that it was unjust and undermined respect for human rights.[173] In December 2004, the House of Lords found that the provisions that allowed the detentions were illegal (See Resisting the Registration and Surveillance Agenda, p.).

In Canada, as of December 2004, at least six men were being detained indefinitely without charge under "security certificates" issued by the Minister of Public Safety and Emergency Preparedness and the Minister of Citizenship and Immigration.[174] The Canadian *Anti-Terrorism Act* provides authorities with additional power to detain people without charges using "preventative arrests".[175]

e) Broad Strokes: The U.N. List

As the mass detentions carried out by the U.S. described above show, low-tech risk assessment, like high-tech risk assessment, often cuts a broad swath. This can also be seen in the list of names compiled pursuant to U.N. Security Council Resolution 1373, which calls on states to freeze the assets of terrorists or those supporting them.

It is not known whether there are any criteria for the list; if there are, they are not public. If they exist, the story of Liban Hussein suggests the criteria must be very loose. On November 7, 2001, the U.S. government issued a list of 62 people and businesses whose assets were to be frozen. In a speech that day, President Bush said there was clear evidence that the people on the list were the "quartermasters of terror".[176] The U.S. list was then adopted by the U.N. in its list for freezing assets, and by other U.N. member states including Canada. Shortly thereafter, the Canadian government froze the Canadian assets of Liban Hussein, a Somali-born Canadian businessman who ran a money transfer business in Dorchester, Massachusetts and whose name was on the U.S. and U.N. lists.[177]

Canada jailed Hussein briefly, made it a crime for anyone to do business with him, and took steps to have him deported to the U.S. Then in June 2002, proceedings against him were abruptly terminated when the Department of Justice admitted that further investigation had revealed no evidence to suggest he had anything to do with terrorism. After having devastated the man's business, the Canadian government removed his name from its list for freezing assets and settled out of court with him. Eventually his name was removed from the U.S. and U.N. lists as well.[178]

Reportedly, there are a number of people on the U.S. list who, like Liban Hussein, run *hawalas*. *Hawalas* are traditional, informal money-transfer businesses which Somalis use to send money to Somalia, since the normal banking system there collapsed in the early 1990's. Around two thirds of the money transferred to Somalia is sent through *al-Barakaat*, one of the largest hawalas. In Sweden, authorities froze the accounts of three organizers of *al-Barakaat,* Swedish citizens of Somali origin, in order to comply with the E.U. and U.N. lists. But because the three were so obviously innocent, a public campaign started up and quickly raised 22,000 euros for the men's basic needs. Lawyers for the three men met with the European Commission, the European Parliament and the U.N. Committee on Human Rights and also lodged a case at the European Court.

At no time throughout the affair did the U.S. present any evidence or specific accusations against the three men. To have their names removed from the lists they were ultimately forced to sign a statement for U.S. authorities saying that they had never been and never would be involved in the support of terrorism and would immediately cease all contacts with *al-Barakaat*. A joint request from Sweden and the U.S. to the U.N. Sanctions Committee then resulted in a decision to remove their names from the various lists. A Swedish parliamentary inquiry concluded that although the government should have reacted much earlier, and at the very least asked questions before implementing the U.N. and E.U. lists, it had not had many options, due to its obligations in international law.[179]

f) Disciplining Dissent

In the low-tech version of risk assessment, governments often give way to an impulse to punish dissent.

i) Targeting the "Unpatriotic" in the U.S.

The American Civil Liberties Union (ACLU) and newspapers across the United States have

documented numerous instances in which U.S. authorities have made extremely questionable risk assessments, targeting citizens who have criticized the policies of the Bush Administration.[180] This is partly the fault of the definition of "terrorist" in the *USA PATRIOT ACT*, which is so broad that it sweeps in legitimate activities of dissent. But the targeting of dissenters is also happening because a climate exists in times of danger in which there is enormous pressure to conform to what is viewed as "normal" and "patriotic" behaviour – and an enormous tendency to engage in a "circling of the ideological wagons" and a collective witch hunt for the "enemy within".

Richard Bourne, a social critic during another highly polarized time in American history, the First World War, reflected that war "… automatically sets in motion throughout society those irresistible forces for uniformity, for passionate cooperation with the Government in coercing into obedience the minority groups and individuals which lack the larger herd sense."[181] In such a time it can be dangerous to be "different", or to exercise that quintessential right of American democracy, the right to dissent.

A Senate committee, reporting on the elimination of restrictions on the F.B.I.'s ability to surveil U.S. citizens, wrote that the agency. had adopted the "belief that dissident speech and associations should be prevented because they were incipient steps towards the possible ultimate commission of an act which might be criminal".[182] In the same vien, a spokesperson for the California Anti-terrorism Information Center, has evinced the belief that dissenters from the "war on terror", and the war on Iraq in particular, could well be characterized as terrorists:

> "If you have a protest group protesting a war where the cause that's being fought against is international terrorism, you might have terrorism at that [protest]. You can almost argue that a protest against that [war] is a terrorist act."[183]

Many of the instances documented by ACLU and journalists involve people protesting the war in Iraq. In spring 2004, for example, the F.B.I. served a subpoena on Drake University regarding an anti-war conference that was held there.[184] In 2003, New York police questioned anti-war protesters about their political activities and associations.[185]

But other dissenters from Bush Administration policies have also been targeted. In October 2001, A.J. Brown, a 19-year-old freshman nearly jumped out of her skin when the U.S. Secret Service knocked on her door. They had received an anonymous report that Brown had an "anti-American" poster in her student digs. Did she have any information about Afghanistan? No. About the Taliban? No. Only a poster opposing the death penalty, which showed George Bush holding a rope in front of rows of hanged corpses, with the caption, "We hang on your every word".[186]

ii) The U.S. "No Fly" List

The names of peace activists, civil libertarians, Quakers, and a satirical cartoonist have shown up on the U.S. on the "no fly" list, the "low-tech" version of the high-tech CAPPS II/ Secure Flight passenger screening program (see p. __).

Jan Adams and Rebecca Gordon were pulled aside in San Francisco International Airport and told they could not board their flight because their names appeared on the list. The two women, who are peace activists and publish a newspaper called *War Times*, were not told how their names got on the list or how they could have them removed. There appeared to be no reason for their inclusion on the list,

other than the fact that they had been exercising their right to disagree with the government. An ACLU lawyer, a retired Presbyterian minister, a man who works for the American Friends Service Committee (a Quaker organization whose purpose is to promote peace and social justice), and an ACLU special projects coordinator[187] have also been among the many passengers pulled aside under the U.S. "no fly" list. In Canada, Shaid Mahmoud, a Toronto editorial cartoonist who has been critical of U.S. and Israeli foreign policies, was refused the right to buy a ticket by an Air Canada agent because his name appeared on the U.S. list.[188]

The "no fly" list is run by the Transportation Security Administration, with names fed to it by the F.B.I. and intelligence agencies. Airlines are required to stop passengers whose names appear on the list from flying, or to subject those identified as "selectees" to more rigorous security screening. Despite requests under the American *Freedom of Information Act*, there has been no disclosure of the purpose of the list, or the criteria for adding names to it.

Once a person's name appears on the list, there seems to be no established procedure for removing it. Massachusetts Senator Ted Kennedy was stopped from getting on a plane from Washington to Boston by a ticket agent who reportedly saw his name on the "no fly" list. Eventually Kennedy was allowed to fly home, but he was stopped again on the return journey to Washington. In order to get his name removed from the list he had to to enlist the help of Homeland Security Secretary Tom Ridge[189] Dozens of men with the misfortune to be named David Nelson have been questioned by ticket agents, pulled off planes and interrogated.[190]

In September 2004, Canada admitted it was in the process of establishing its own "no fly" list pursuant to the new *Public Safety Act*. However, in October 2004 the Minister of Transport noted that the initiative was far from being established because of the many legal considerations it raised, including the guarantee of free mobility in the *Charter of Rights and Freedoms* and federal privacy laws that limit distribution of personal information.[191]

iii) Open Season on Individuals and Groups Challenging Repressive Regimes

In repressive regimes, the risk assessment model being applied in the "war on terrorism" has allowed authorities to comfortably declare an open season on dissidents and groups challenging their power. PEN International has reported that in Burma, China, Colombia, Democratic Republic of Congo, Indonesia, Jordan, Pakistan, Turkey and other countries, authorities have "[found] that defining their opponents as 'terrorist sympathizers' is a convenient way of stifling opposition movements".[192] In Tunisia, the lawyers of individuals charged with terrorism have themselves been charged with terrorism.[193] In India, individuals protesting the clearing of land for a business development have been prosecuted under antiterrorism legislation. In Eritrea, independent newspapers have been shut down and their journalists jailed after being accused of having terrorist ties. In Uzbekistan, members of the Human Rights Society have been jailed on weak evidence alleging they recruited Islamic militants. In Colombia, President Andres Pastrana has said that rebels in a four decade civil war would be treated as terrorists "[a]nd in that, the world supports us."[194]

On can imagine how much easier it will be for these regimes to punish dissenters and opponents with the greater surveillance capabilities and support from other countries they will have under the new global infrastructure for mass surveillance.

g) A Plethora of Ballooning Watch Lists

In low-tech risk assessment, watch lists proliferate and they are often as dangerously flawed as the watch lists created by high-tech methods.

In addition to the U.N. list, and the "no fly" list described above, a plethora of low-tech lists have sprung up since 9/11.

Myth #5: Terrorist watch lists are a reliable product of international intelligence cooperation and consensus.

None of these lists was the product of objective, careful international agreement. Even the U.N. list is a compilation of national products of variable reliability (see p.). In many countries the definition of "terrorism" used to create lists is so vague that, as the former Director of the Canadian Security Intelligence Service has said of the Canadian definition, it "…could easily include behaviour that doesn't remotely resemble terrorism".[195]

Opponents of a repressive regime in a liberation movement or civil war could be labeled "terrorists" under many countries' definitions of terrorism, even though they are not targeting civilian populations. In fact, the U.S. Military Commission Instruction No. 2 on "Crimes and Elements for Trials by Military Commission" and its Comments, for example, define the offence of "terrorism" as including "an attack against a military objective that normally would be permitted under the law of armed conflict"![196]

There is no due process afforded individuals or groups to allow them to challenge the inclusion of their names on a list. And, once the "terrorist" label is fastened to them, actions are taken against them without normal legal protections being afforded (protections such as presumption of innocence, the right to know the evidence and allegations against one and to respond, the right to remain silent, and habeas corpus). This is the essence of the risk assessment model: it treats as intolerable risks the very legal protections that are fundamental to free and democratic societies.

In the U.S. there were, until recently, nine agencies administering twelve different watch lists. Each of these watch lists was created for a different purpose, using different criteria. The government has enough information to justify suspicions that some of the people on these lists are dangerous. Others are suspected of being dangerous, but the evidence is thin. Others should simply not be on any list: they are there because of some misspelling of their name, or on the basis of some mistaken assumption about their background, or due to crude ethnic and religious profiling, or because they have been critical of the government, or because some state agent decided that he or she would rather be "safe than sorry".[197] The F.B.I. stopped Air France and British Airways flights to the U.S. in late 2003, based on matches with names on terrorist lists. The suspects turned out to be a five year-old child with a similar name to a wanted Tunisian, a Welsh insurance salesperson, an elderly Chinese woman, and a prominent Egyptian scientist. "A check was carried out in each case and in each case it turned out to be negative," a spokesman for the French Interior Minister said, "the F.B.I. worked with family names and some family names sound alike."[198]

In short, the U.S. lists have "been created haphazardly and without the carefully constructed checks and balances that such powerful instrument[s] demand."[199] And the lists are certainly bloated. At various

times, news reports have put the numbers of names on the U.S. lists in the millions.[200]

Recently, a Terrorist Screening Center was created in the U.S., under the lead of the F.B.I., to merge the lists.[201] However, critical questions remain to be resolved. Who will have the authority to add names to the list, using what criteria, and for what purpose? How will the F.B.I. allow individuals to know if they are on the list, address the lack of due process for individuals wrongly included on the list, maintain the accuracy of the list, and ensure that authorities identifying someone on the list know why that person is on the list and what action is appropriate to take? How will information be shared among agencies, and will private companies have access to it?

To date, there has been a troubling involvement of the private sector with the watch lists. As with the surveillance of electronic communications (see p.), private organizations and corporations are being turned into the agents of the state. Under a program called "Project Lookout", the F.B.I. circulated a list of hundreds of names to corporations. The list, which was full of inaccuracies and contained the names of many people with whom the F.B.I. simply wanted to talk, was widely shared and quickly took on a life of its own.[202] Health insurance giants looked through millions of customer records. Blue Cross found no terrorists, but 6,000 false positives (out of 6 million records) were generated, all of whom were investigated further by the company's employees. Aetna searched through 13 million records. The F.B.I. admitted it had no way to remove innocent people from the list, because its distribution had spun out of its control.[203]

As mentioned earlier, financial companies (under s. 326 of the *USA PATRIOT ACT*), and businesses involved in helping individuals to buy or sell property, (under Executive Order 13224) must verify each customer's identity and then check whether the person is on a government watch list (see p.).[204]

3. Kafka

The post-9/11 world of "risk assessment" – whether one is experiencing the "high-tech" version or the "low-tech" version – is Kafkaesque.[205]

It is a world in which individuals are presumed guilty, detained and not told the charges against them, denied the right to face their accusers, denied the right to know the evidence against them and the criteria by which they are being judged, and given no legal recourse and no one to advocate for them.

SEVENTH SIGNPOST: DEEP INTEGRATION AND THE LOSS OF SOVEREIGN CHECKS AND BALANCES

When all the initiatives described above are viewed together, what emerges are the "contours of a vast, increasingly integrated multinational registration and surveillance system, with information floating more or less freely between subsystems".[206]

As this system emerges, the police, security intelligence, and military operations of many nations are becoming deeply integrated with U.S. operations. National governments are giving up sovereignty and throwing aside national checks and balances in favour of an integrated security space that is largely being designed and controlled by the U.S.

Myth #6: If one is mistakenly caught up in the global mass surveillance net, one's government can protect one.

As a result, when the U.S. government takes aggressive action against the citizen of another country on the basis of information shared by that country's officials, there is little the citizen's government can do to protect him or her. This was painfully evident in the Arar case, when the Canadian government was unable to secure the release of Maher Arar for months, even after meetings at the highest levels with U.S. and Syrian officials.[207]

Governments' inability to protect their citizens was also apparent when the Swedish government sought to have several of its citizens' names removed from the U.N. list after they had been added at the request of the United States. As mentioned earlier (see p.), the Swedish government had to negotiate with the U.S. government in order to have the names removed. Its citizens, who were of Somali origin, were forced to sign a statement for U.S. authorities swearing that they never had supported and never would support terrorism, and that they would cease all contact with the hawala, al Barakaat.[208]

Myth #7: Governments want to implement these systems to protect their citizens from terrorists.

There are various forces at work driving deep integration with the U.S. There is certainly some belief among governments that better sharing and cooperation among states is necessary in order to effectively counter international terrorism. However, many of the agreements and arrangements made are irresponsible in terms of the sovereign powers they cede and the lack of adequate conditions and controls they contain regarding the sharing of information.

Some of the willingness of governments to acquiesce to the integrated security space demanded by the U.S. is rooted in opportunism. U.S. bilateral demands and those channelled through international forums give governments the excuse to do what they otherwise might not be able to do – to increase their social control within their own borders. This is the eternal tendency of governments and law enforcement, and it is the reason why democracies have entrenched rights and other institutional checks and balances.

In many cases, however, economic interests also drive governments to acquiesce to the integrated security space being pushed by the U.S. The E.U., for example, feared the economic consequences of its airline industry being denied landing rights in the U.S. when demands for PNR sharing were made; this was part of what led it into negotiations for a formal agreement on PNR sharing.[209] In Canada, where 30 percent of the economy depends on exports to the U.S.,[210] where a border open to the flow of export traffic is critical, and where powerful business interests have been lobbying for yearsfor deep integration with the U.S.,[211] the government was quick to negotiate a *Smart Border* agreement and *Action Plan* (see page) that were, in essence, a blueprint for many of the initiatives described above.

Many other countries that depend on trade with, or aid from, the U.S. have found themselves in similar situations. Southeast Asian governments, especially those of the Philippines, Singapore, Thailand, Malaysia and Indonesia, have cooperated closely with the U.S. in its global campaign against terrorism. The collaboration ranges from arresting alleged terrorists based on shared intelligence and allowing U.S. agents to interview detainees, to facilitating the extradition of detainees to the U.S., to legislating anti-terror laws to serve the U.S.-led anti-terrorism campaign,[212] to allowing U.S. military forces to lead special operations against terrorist groups in the country.[213] The E.U. is also putting pressure on countries, through aid, to cooperate with the

security agenda it shares with the U.S. In March 2004, E.U. foreign ministers backed a declaration warning countries that they would lose aid and trade with the powerful economic bloc if their efforts in security cooperation were deemed insufficient.[214]

The benefits of deep integration and a single security space for the U.S. include the opportunity to advance its hegemonic interests in strategic regions. For example, years of U.S. military presence were ended in the Philippines as a result of popular protest, but the U.S. reasserted its military presence after 9/11. This was done, ostensibly, to assist in the capture of Philippine-based terrorists, which would ordinarily be a law enforcement function of the Philippine state. But it was done without a treaty or even the usual "status of forces" agreement, and represents one of the extremes on the continuum of deep integration.[215]

EIGHTH SIGNPOST: THE CORPORATE SECURITY COMPLEX

In Dwight Eisenhower's farewell address at the end of his presidency in 1961, he warned the American people about the rise of a powerful military industrial complex that threatened the foundations of American democracy:

> This conjunction of an immense military establishment and a large arms industry is new in the American experience. …The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted.[216]

Today, the same warning could be made with respect to the new symbiotic relationship that is developing between an immense security/intelligence establishment and an ambitious information technology industry. This new *corporate security* complex is an aggressive driver of the project for global, mass registration and surveillance.

For information technology corporations, the paradigm of the "war on terror" is a boon after the sector's disastrous economic downfall in the mid-to-late 1990s. It offers them a critical opportunity for recovery and expansion, and they have been quick to seize it – setting in motion a powerful lobby to promote technological solutions for governments that purportedly "increase" security and "eliminate" risks.

For the government security/intelligence community, left searching for a *raison d'être* after the end of the Cold War, the "war on terror" offers an unprecedented opportunity to increase its investigative and surveillance powers by tapping into the possibilities offered by new information technologies. And many of these technologies are owned or being developed by the private sector.

However, the private sector offers something more than technology to government agencies: it offers a way around some of the laws and accountability mechanisms that govern government agencies. For example, contracting with private data aggregation corporations allows government agencies to access massive databases of personal information they would not, under privacy and other laws, be able to maintain themselves. Contracting with private corporations for the development of data mining projects similarly allows government agencies to evade privacy. To some degree, it also allows governments to shield the projects from public scrutiny.

Billions of dollars, euros, and other currencies fuel the corporate security complex.

In the U.S., an estimated $115 billion was allocated for research and development of anti-terror initiatives in 2003 alone. The estimated

allocations up to 2010 are $130 billion to $180 billion a year.[217]

A security research program announced by the E.U. in February 2004 is intended to make the E.U. the rival of the United States in security technology. This "comprehensive" research program is aimed explicitly at building a "security culture" in Europe with the help of the "security industry and the research community". The program is charged, among other things, with:

> [demonstrating] the appropriateness and acceptability of tagging, tracking and tracing devices by static and mobile multiple sensors that improve the capability to locate, identify and follow the movement of mobile assets, goods and persons, including smart documentation (e.g. biometrics, automatic chips with positioning) and data analysis techniques (remote control and access).[218]

This research program is being developed based on the recommendations of a "Group of Personalities" that included representatives of eight multinational companies (including BAE and Siemens) and seven "research" institutions (including the Rand Corporation).[219] By 2007, the European Commission will be providing the security research program with more than a billion euros a year.[220]

In Canada, the government announced a comprehensive $Cdn. 7.7 billion package for security spending over a five-year period in its 2001 budget. The package included substantial spending on surveillance and security technology.[221]

The major surveillance projects promoted to date by the American government – such as the Terrorism [Total] Information Awareness System, MATRIX, US-VISIT and CAPPS II/Secure Flight programs – have provided formidable business opportunities and profits for technology corporations.

Data aggregator companies like Lockheed Martin, Acxiom, Lexis-Nexis, ChoicePoint and others are major winners in these multi million dollar ventures. ChoicePoint alone claims to have contracts with some 35 U.S. government agencies, including a $8 million contract with the Justice Department that allows the F.B.I. to tap into the company's vast database of personal information on individuals. The Georgia-based company increased its lobbying expenditures from $100,000 in 2000 to $400,000 in 2002.[222]

Prior to being forced by Congress to abandon research on TIA in the fall of 2003 (see p.), the Defense Advanced Research Projects Agency oversaw a budget of roughly $2 billion and relied heavily on outside contractors. Between 1997 and 2002, it granted contracts to data aggregator companies worth $88 million. Among these, 13 contracts worth more than $23 million went to Booz Allen & Hamilton, and 23 contracts worth $27 million were granted to Lockheed Martin.[223]

Although TIA was shelved at the federal level, the MATRIX program (see pp . and) has been in the process of implementation at the state level since 2002. As mentioned earlier, it ties together government and commercial databases in order to allow authorities to conduct detailed searches on individuals, and to search for patterns in the databases that are supposedly indicative of terrorist or criminal activity. Maintenance of the system has been contracted out to Seisint Inc., based in Boca Raton, Florida. By the fall of 2003, Seisint had received $12 million in Federal funds to run the system.[224] In January 2003, a presentation about MATRIX was delivered by its promoters to U.S. Vice-President Dick Cheney and other top U.S. officials by Seisint, Florida Governor Jeb Bush and Florida's top police official.[225]

The US-VISIT program (see p.) is another goldmine for the corporate sector. Congress appropriated $368 million in 2003 to develop the system and install it in airports, and $330 million to expand the system to land borders in 2004.[226] In May 2004, the Department of Homeland Security issued a call for bids to extend the system at sites abroad where people seek visas to the United States. Three companies vied for the contract – Accenture, Computer Sciences and Lockheed Martin. [227] Accenture, the winner, could earn as much as $10 billion in the venture by 2014.[228]

Lockheed Martin, a giant of the military industrial complex, received a five-year, $12.8 million contract to assist the Transportation Security Administration in the development of the CAPPS II program (see p.).[229] Before its inauguration was postponed (see p.), more than $60 million had been spent on the development of computer technology intended to verify individuals' identities' against commercial databases.[230]

CAPPS II relied heavily on data and identity-matching logarithms developed by Acxiom. The Little Rock-based company is the world's largest processor of consumer data, collecting and manipulating more than a billion records a day, and is rapidly expanding its reach in Europe and Asia.[231] Since 9/11, Acxiom has been lobbying for federal contracts in homeland security with the help of retired general and presidential candidate Wesley Clark and Bill and Hillary Clinton. Clark has also lobbied on behalf of Lockheed Martin. In February 2003, the TSA made Lockheed Martin its main contractor on CAPPS II, and Acxiom obtained an important subcontract.[232]

Biometric passports and the US-VISIT program aim to biometrically identify the world's passport holders, and this also offers the prospect of huge profits for corporations globally. The contract awarded by the Swedish government to Setec, a Finnish company, to supply biometric passports and ID cards over the next five years is worth 100 million euros.[233] Another lucrative contract with the Danish government will see Setec provide three million Danes with biometric passports.[234]

In Canada, ACME-Future Security Control, an Ottawa-based company, was chosen by the Canadian Air Transport Security Authority to develop a secure credential card, using biometric technologies, for individuals accessing restricted areas of airports.[235]

In Asia, the Indian smart card industry is growing at a rate of 45% annually, and will be worth $6 billion (U.S.) by 2010 and companies like Sony, Infineon and Hitachi are "licking their lips".[236]

IT corporations, such as Oki, have recently moved into the biometrics sector, anticipating its potential. Oki now specializes in iris scans and is working for the German government on a pilot project in the Frankfurt airport.[237] Corporations that specialize in biometrics, such as Byometric Systems (Germany), Bioscrypt (Canada) and BioDentity (Canada), are aggressively looking for a piece of the anti-terrorism action. On its website, BioDentity quotes a Frost & Sullivan claim that "[c]utting-edge security systems could have prevented the catastrophe – the worst terrorist attack in U.S. history".[238]

Corporations have been quick to seek relationships globally with security apparatuses. SITA Information Networking Computing, an IT company registered in the Netherlands, is now implementing "intelligent border services" in Bahrain, Australia and New Zealand, including a tracking system that analyzes the travel patterns of high risk passengers.[239] Siemens, a company based in Germany, is now providing passports to the U.K. government, national ID

cards with chips and biometrics to Macau, ID cards to Bosnia-Herzegovina and Italy, and visas to Norway.[240] In 2002, the France-based Thales Group sought and won the contract for the Chinese ID card.[241] In September 2004, the Canadian government facilitated the mission of a Canadian trade delegation to China to promote the sale of surveillance and security technology to the Chinese government, including closed circuit television devices, night-vision products, face recognition technology and computer systems for monitoring the Internet.[242]

In the fray of all the activity described above, corporations are constantly "pushing the envelope" of social control by technological means – egging on governments to embrace bigger, newer, and more intrusive systems of social control.

It is not implausible in the new world order that corporations will sell governments on the idea that their populations should be required to have computer chips implanted under their skin, so that the state may better control them. In October 2004, the U.S. Food and Drug Administration authorized Applied Digital Solutions, a Florida-based company, to market implantable chips for patients that will encode their medical records. The company expressed the hope that the medical use of its VeriChips would accelerate the acceptance of under-the-skin ID chips as security and access control devices.[243]

Eisenhower's warning that we should take nothing for granted, it would appear, has never been more relevant.

NINTH SIGNPOST: THE EXPROPRIATION OF THE DEMOCRATIC COMMONS

The global project for mass registration and surveillance that governments and corporations are building in the name of protecting freedom and democracy is, in fact, threatening those very values around the world. In the North and in the South, the East and the West, the democratic "commons" that have been won after centuries of struggle are being expropriated. Misguided governments pushing to implement the global surveillance project are:

• suspending judicial oversight over law enforcement agents and public officials;

• placing unprecedented power in the hands of the executive arm of government;

• making end-runs around the oversight and debate normally provided by the legislative arm of government;

• inviting unelected, unaccountable supranational bodies to set policy for them;

• abandoning well-established privacy protections for citizens;

• ignoring constitutional guarantees;

• rolling back criminal law and due process protections (such as the presumption of innocence, *habeas corpus*, solicitor-client privilege, public trials, the right to know the evidence against one and to respond, reasonable grounds for search and seizure, and the right to remain silent) that balance the rights of individuals against the power of the state;

• systematically violating basic human rights; and

• endangering the rule of law itself.

Governments have been able to make these changes in democratic countries by declaring a state of crisis. But the "war on terror" is a war without end, so the state of crisis is permanent, not temporary. As a result, democratic societies are in grave danger of being turned, over time, into surveillance societies – or worse, into police states.

In undemocratic societies, the prospects for freedom are fading. Emboldened by the abandonment of democratic values in Western countries, governments in these countries are abandoning democratic reforms and tightening their grip on power. In Russia, for example, President Vladimir Putin announced, in September 2004, plans for a sweeping political overhaul in the name of fighting terrorism. If adopted as expected, his controversial proposals will strengthen the president's already extensive control over the legislative branch and regional governments.[244]

In the 18th century, English philosopher Jeremy Bentham proposed an architectural design for what he considered the perfect prison. It enabled one unseen warden to watch all of the prisoners in an institution. Bentham called his design the "Panopticon". His idea was that if prisoners never knew when they were actually being watched – only that they might be watched at any time – they would begin to modify their behavior. Fearing they could be seen, and fearing punishment for transgressions observed, they would begin to internalize the rules of the institution so that actual punishment would eventually be rendered superfluous.[245]

As people begin to realize that every transaction in their personal lives is potentially being watched – and that their innocent actions and beliefs can be easily misconstrued by risk assessors in their own and other countries, they will begin to internalize the social control that is being exerted by governments, watching what they say, what they criticize, who they associate with, and what they profess to believe in.

French philosopher Michel Foucault wrote that:

> In appearance [panopticism] is merely the solution to a technical problem, but, through it, a whole new type of society emerges [transported] from the penal institution to the entire social body.[246]

TENTH SIGNPOST: A LOSS OF MORAL COMPASS – RENDITION, TORTURE, DEATH

One commentator, reflecting on the implications of writing about biometric registration and mass surveillance, has written:

> There has been an attempt the last few years to convince us to accept as the humane and normal dimensions of our existence, practices of control that had always been properly considered inhumane and exceptional.[247]

To this observation, it could be added that once societies begin to accept inhumane and exceptional practices of social control, they begin to lose their moral compass.

It is now clear that the U.S. and other countries participating in the global surveillance project are engaging in torture, inhumane treatment, and indefinite detention of detainees of the "war on terror" in their own facilities, as well as sending suspects to third countries where they face torture, inhumane treatment, and indefinite detention. So that the worst that individuals have to fear from the global system of mass surveillance is something far darker than "mere" loss of privacy, civil liberties, freedom of movement, or loss of democratic patrimonie: that is, that the system runs alongside and feeds into what some commentators are calling a global gulag.

1. The Global Gulag

a) Detention Centres Used by the U.S.

When Alexander Solzhenitsyn wrote *The Gulag Archipelago* in the last half of the 20th century, he described a physical chain of island prisons clustered in Soviet Russia's northern seas and Siberia. But the description was metaphorical as well as physical: the archipel-

ago was a cluster of prisons around which swirled the sea of normal society.[248] Before and during Solzhenitsyn's time, people were often sent to the gulag secretly, without due process, and many disappeared, never to be seen again.[249]

Like the Russian system that Solzhenitsyn described, the United States is operating an archipelago of prison camps and detention centres around the world that remains largely unseen by the world. Some of these are being run directly by the U.S. – including Camp Delta at Guantanamo Bay in Cuba; Bagram and other military bases in Afghanistan; Camp Justice on British Diego Garcia; a floating detention centre on board a U.S. naval vessel in the Indian Ocean; Camp Cropper at the Baghdad airport and other detention centers in Iraq; the U.S. airbase in Qatar; a jail with an undisclosed location referred to by the C.I.A as "Hotel California"; and other C.I.A. centres disclosed and undisclosed in Afghanistan, Pakistan, Thailand, Jordan, Qatar, and elsewhere.[250]

Other detention centres are run by allies of the U.S. in its "war on terror", in close cooperation with U.S. agencies like the C.I.A.. These centres are located in Jordan, Syria, Egypt, Morocco, Saudi Arabia, Uzbekistan, and Pakistan — countries with documented records of using torture in interrogation and indefinite detention.[251] Among the worst are the Far' Falastin interrogation centre in Damascus, Syria, where Maher Arar was held, and the Scorpion jail and Lazoghly Square secret police headquarters in Cairo.[252] Former C.I.A. agent Bob Baer, who worked covertly for the U.S. across the Middle East until the mid 1990s has said, "If you want a serious interrogation, you send a prisoner to Jordan. If you want them to be tortured, you send them to Syria. If you want someone to disappear – never to see them again – you send them to Egypt."[253]

Although difficult to verify, Pentagon figures and estimates of intelligence experts put the number of people being held by the U.S., directly or at its request, at more than 9,000 as of May of 2004.[254]

b) The Practice of Rendition

Many detainees have been transferred to detention centres in other countries from the Afghan and Iraq[255] theatres of war, in contravention of Art. 49 of the *Fourth Geneva Convention*, which provides that "[i]ndividual or mass forcible transfers, as well as deportations of protected persons from occupied territory to the territory of the Occupying Power or that of any other country ... are prohibited, regardless of their motive". However, the Bush Administration has also moved detainees to and between detention centres using an existing American practice known as "extraordinary rendition".

The practice was developed as "rendition to justice" in the late 1980s, reportedly to allow U.S. agents to apprehend wanted persons in failed states like Lebanon,[256] where lawful extradition procedures were either ineffectual or non existent. Before September 2001, the C.I.A. was authorized by presidential directives to carry out renditions, but the rules were restrictive, requiring review and approval by interagency groups led by the White House. The purpose of the procedure at that time was to bring prisoners to the United States or to other countries to face criminal charges.[257]

According to current and former government officials, days after September 11, 2001, President Bush signed a directive that gave the C.I.A. expansive authority to use rendition *without* case-by-case approval from the White House, the State Department, or the Justice Department.[258] Since then, the program has "expanded beyond recognition – becoming, according to one former C.I.A. official, 'an

abomination'".[259] Rendition is now being used – not to bring a small number of individuals charged with criminal offenses to face trial in the U.S. – but to transfer a large group of individuals who will likely never have criminal charges brought against them to detention centres outside of the U.S., and solely for the purpose of detention and interrogation.[260] As another C.I.A. official has said of the current practice, "It's not rendering to justice. It's kidnapping."

This new form of rendition has become one of the principal strategies of the U.S. in the "war on terror".[261]

Under the new form of rendition, the United States picks up individuals around the world with the help of its allies, and transfers them to extraterritorial detention camps and centres on jets operated by the U.S. Special Collection Service. The service runs a fleet of luxury planes and military transports that has moved thousands of prisoners around the world since September 11, 2001 – much as the C.I.A.'s secret fleet, "Air America", did in the 1960s and 70s.[262] Maher Arar was transported to Jordan (on his way to Syria), in this way.

c) Disappearance

The operations of the Special Collection Service air fleet, and of the detention centres to which it delivers detainees, are shrouded in secrecy.[263] With few exceptions, when detainees arrive at their destinations either as rendered suspects or as prisoners captured in a theatre of war, they disappear.

The *Geneva Conventions* require the prompt registration of detainees captured in theatres of war, so that their treatment can be monitored.[264] Under the Rome Statute of the International Criminal Court, "enforced disappearance" is a "crime against humanity" and is defined as "the arrest, detention or abduction of persons by, or with the authorization, support or acquiescence of, a State or a political organization, followed by a refusal to acknowledge that deprivation of freedom or to give information on the fate or whereabouts of those persons, with the intention of removing them from the protection of the law for a prolonged period of time."[265] While the U.S. is not a signatory to the Rome Statute, the Statute's definition arguably codifies existing international law regarding disappearances.

Although the U.S. has released the names of a few of the high level Al Qaeda suspects it holds,[266] and other detainees' names have become public through families' efforts as in the case of Maher Arar, the U.S. does not release any details about the people it renders to foreign prisons[267] or about most of the people the people it holds in C.I.A.-run detention centres.[268] The latter have been called "ghost detainees" by Human Rights Watch, since the Bush Administration has consistently refused to reveal their fate or locations.[269] Recent additions to their ranks came from the Iraq theatre of war when a number of detainees were kept off the registers shown to the Red Cross there with the approval of the U.S. Secretary of Defense, Donald Rumsfeld.[270]

As of March 2005, the Bush Administration was still refusing to release the names of detainees held at Guantanamo Bay to lawyers and the public — seven months after the U.S. Supreme Court's ruling in *Rasul v. Bush*[271] which held that every detainee there had the right to challenge his detention in federal court. Most of these detainees were transferred from the Afghan theatre of war but many have been rendered there from other countries.[272]

In 2002, at a joint hearing of the House and Senate Intelligence Committees, Cofer Black, then Head of the C.I.A. Counterterrorist Center, spoke of the United States'new forms

of "operational flexibility" in dealing with suspected terrorists: "This is a highly classified area. All I want to say is that there was "before 9/11", and "after" 9/11. After 9/11 the gloves come off."[273]

d) The Assertion of a Legal Black Hole and Authority to Torture

The Bush Administration has asserted that neither the U.S. Constitution,[274] nor the *Geneva Conventions*, [275] nor international human rights law[276] apply to "enemy" or "unlawful combatants" in the "war on terror". In other words, according to the United States, these detainees exist in a legal "black hole". They are in a no man's land where the United States, and by implication its allies, are free to act outside the law, or to pick and choose what parts of the law they will apply – as in the Military Orders and Instructions[277] for the detainees in Guantanamo Bay.

While there is some basis in U.S. caselaw to suggest that the U.S. Constitution does not apply to aliens outside the U.S.,[278] the Administration's assertions in respect of the *Geneva Conventions* and human rights obligations are false. Under the *Geneva Conventions* there is no such category as "enemy" or "unlawful" combatant. In armed conflict like the war in Afghanistan or the war in Iraq, all persons are covered under the *Conventions* either as "civilians" or "combatants".[279] In respect of human rights law, under the *International Covenant on Civil and Political Rights* (to which the U.S. is a signatory) states arguably bear obligations wherever they have jurisdiction.[280] Under the *Convention Against Torture* (to which the U.S. is a signatory) states are responsible for taking effective legislative, administrative, judicial, and other measures to prevent acts of torture in any territory under their jurisdiction.[281] Finally, it is clear that, under the customary international law of human rights the detainees have due process rights and protections against torture, arbitrary and prolonged detention, and extra judicial killing.[282]

The Bush Administration has repeatedly denied that it condones the torture of detainees or that it has a policy of torture, but evidence suggesting the contrary is mounting.

The American newsmagazine *Newsweek* has reported that after September 11, 2001, President Bush signed a secret order authorizing the C.I.A. to set up detention centres outside the U.S. and "to question those held in them with unprecedented harshness".[283] According to *Newsweek*, agreements were then negotiated with foreign governments with respect to these sites, giving U.S. personnel and private contractors immunity for their actions there.[284]

Newspapers have also reported on a series of internal legal memoranda, collectively referred to as "the torture memos". These memoranda, some of which were leaked and some of which were made public by groups such as the N.Y.U. Center for Law and National Security, advise the Bush Administration, in essence, on how to engage in practices of inhume treatment and torture, and justify or redefine the conduct. According to the *New Yorker*, most of the memoranda "were generated by a small hawkish group of politically appointed lawyers in the Justice Department's Office of Legal Counsel and in the office of Alberto Gonzales". [285] At the time the memoranda were written, Gonzales was White House Legal Counsel. More recently, he has been appointed by President Bush to be the new Attorney General of the United States.

• A series of memoranda written in January 2002 by the Justice Department, provided legal arguments to support Bush Adminstration officials' assertions that detainees captured in the

Afghan theatre of war did not have to be treated in accordance with the *Geneva Conventions*, creating a new category not found in the *Geneva Conventions* — that of "illegal enemy combatant"[286]

• An August 2002 memorandum signed by Attorney General Jay S. Bybee , defined torture as the intent to inflict suffering "equivalent in intensity to the pain accompanying serious physical injury, such as organ failure, impairment of bodily function, or even death." According to newspaper reports, the memorandum "also claimed that torture only occurs when the intent is to cause pain. If pain is used to gain information or a confession, that is not torture."[287] These definitions of torture, of course, do not accord with international law.[288] But a senior Administration official is reported to have said that the memorandum's conclusions align closely with the prevailing White House view of interrogation practices.[289]

• Another memorandum advised interrogators on how to shield themselves from liability under the *Convention Against Torture* and the federal *Anti Torture Act,* by contending that prisoners were in the custody of another government and that U.S. officials were only receiving information from the other country's interrogations.[290]

• A memorandum prepared by a Defense Department legal task force drew on earlier memos to declare that the President could override international treaty prohibitions and federal anti torture law under his authority as Commander-in-Chief to approve any technique necessary to protect the nation's security. The memorandum also stated that Executive and military officials could be immune from domestic and international prohibitions against torture for a variety of reasons, including a belief by interrogators that they were acting on orders from superiors "except where the conduct went so far as to be patently unlawful".[291] This advice contradicts the *Convention Against Torture* which states that "[n]o exceptional circumstances whatsoever … may be invoked as a justification of torture", and, in particular, that "[a]n order from a superior officer or a public authority may not be invoked as a justification of torture."[292]

• According to the *Times*, "a secret memo issued by Administration lawyers authorized the C.I.A. to use novel interrogation methods – including "water-boarding", in which a suspect is bound and immersed in water until he nearly drowns."[293]

• A memorandum from Secretary of Defense Donald Rumsfeld to General James T. Hill of April 2003 outlined permitted interrogation techniques for detainees in U.S. custody, which included stress and duress methods.[294]

• Finally, an F.B.I. email released in December 2004 under a *Freedom of Information Act* request repeatedly referred to an Executive Order that permitted military interrogators in Iraq to place detainees in painful stress positions, to use hoods, to intimidate detainees with military dogs, and to use other coercive methods.[295]

After the Abu Ghraib scandal in Iraq, the August 2002 memorandum described above was formally rescinded by the Justice Department and replaced by a legal opinion that stated torture should be more broadly defined.[296] However, the Bush Administration has fought vigorously against legislative efforts to rein in the C.I.A. In early 2005, "Republican leaders, at the White House's urging, [blocked] two attempts in the Senate to ban the C.I.A. from using cruel and inhumane interrogation methods. An attempt in the House to outlaw extraordinary rendition, led by

Representative Markey, also failed".[297] In fact, as of March 2005 the Administration was supporting a provision in an intelligence reform bill that would authorize U.S. authorities, retroactively, to send foreigners suspected of having links with terrorist organizations to countries where they are likely to be tortured or abused. The provision violates the *Convention Against Torture* which prohibits states from sending persons to countries where there are grounds to believe they would be in danger of being subjected to torture,[298] in that it shifts the burden of proof to the detainee and raises the standard of proof to "clear and compelling evidence" that torture would occur.[299]

e) Torture Committed by U.S. Personnel

In U.S. detention centres, prisoners have been doused with cold water and subjected to freezing temperatures,[300] beaten,[301] denied medical treatment,[302] subjected to severe sleep deprivation,[303] bound in awkward, painful positions for hours,[304] blind-folded and thrown against walls,[305] forced off bridges,[306] subjected to loud continuous music and noises,[307] shot,[308] forced into asphyxiation,[309] water-boarded,[310] had their 7 and 9 year old sons picked up to induce them to talk,[311] been covered with their own urine,[312] strangled,[313] had lighted cigarettes put in their ears,[314] been chained in the fetal position for 24 hours or more,[315] humiliated by female personnel,[316] bitten by dogs,[317] banged headfirst repeatedly into doors,[318] forced to sodomize themselves,[319] held naked for long periods,[320] and thrown on top of each other and jumped on.[321] Military pathologists have pronounced as homicides the deaths of two prisoners in Afghanistan, but in many other cases the military has not conducted autopsies and says it cannot determine the causes of death.[322] As of May, 2004, 39 prisoners had died in U.S. custody in the "war on terror".[323]

A review of this record, alongside the memoranda, Executive Orders, and proposed legislation described earlier, show that the revelations at the Abu Ghraib prison in Iraq which shocked the conscience of the American people in 2004, were by no means an isolated phenomenon. On the contrary, they were part of a wider system of abuse fostered, if not sanctioned, by the top levels of the U.S. government.

f) The Plan to Build Permanent Prisons Outside the U.S.

Michael Scheuer, a counter-terrorism expert with the C.I.A. until 2004, helped establish the practice of rendition. In a recent report he pointed to the folly of the whole project. "Are we going to hold these people forever?"… Once a detainee's rights have been violated you absolutely can't reinstate him into the court system. You can't kill him either. All we've done is create a nightmare."[324]

"A senior U.S. official told the *New York Times* in January 2005 that three quarters of the 550 prisoners then at Guantanamo Bay no longer had any intelligence of value. But they would not be released out of concern that they posed a continuing threat to the U.S."[325] In January 2005, the Washington Post and other newspapers broke the story that the U.S. government was thinking of building jails in foreign countries, "mainly ones with grim human rights records, to which it [could] secretly transfer detainees (unconvicted by any court) for the rest of their lives …. beyond the scrutiny of the International Committee of the Red Cross, or any other independent observers or lawyers."[326]

Under the new scheme, most foreign detainees are expected to be in the hands of the C.I.A., which is subject to less Congressional oversight than other U.S. agencies, operates in secrecy and, as mentioned earlier, gives the Red Cross, lawyers, the media and family no access to detainees.[327] One proposal is for the U.S. to build new prisons in Afghanistan, Saudi Arabia and Yemen. Those countries would run

the prisons but U.S. officials would have access to " monitor human rights compliance".[328] Already, the U.S. has transferred 65 detainees from Guantanamo Bay to other countries, including Pakistan, Morocco, France, Russia and Saudi Arabia so that they can either be prosecuted (an unlikely prospect) or detained indefinitely. The Defense Department has also asked Congress for funds to build a new prison at Guantanamo Bay, since, officials say, any remnant population of detainees that could not be transferred to other countries would likely be held there indefinitely since charges will never be brought against them.[329]

g) The Participation of Other Western Democracies

Myth #8: Western Democracies are defending democracy and human rights around the world.

The new paradigm of having a global pool of detainees held and transferred between centres around the world and accessible to the security agencies of the U.S. and its allies in the "war on terror", is not the policy of the U.S. alone, but is one that is being embraced, acquiesced to, or made use of by many of its Western liberal allies.

The U.K. allows the C.I.A. to operate one of its extraterritorial detention centres on the British island of Diego Garcia. The Swedes have allowed U.S., U.K. and German agencies to question suspects held in Sweden,[330] and have cooperated in the rendition of two asylum applicants from Sweden to Egypt by U.S. agents. Evidence shows that these individuals were tortured in Egypt. One was subsequently released and one was sentenced to 25 years imprisonment by a military court that did not meet international standards for fair trial.

While in a few cases, Western liberal governments or agencies have protested the kidnapping or rendition of their nationals by U.S. agents, the protests have not affected diplomatic relations. In the case of Maher Arar, the Canadian government asked the U.S. government a number of times for his return, and were told it was Canadian agencies which had flagged him to the U.S. as a suspect in the first place. In Italy, police are investigating allegations that U.S. intelligence agents kidnapped an Islamic militant in Milan and transported him in an American plane to Egypt, where he was tortured. Italian prosecutors were angry about his disappearance since they had been preparing to prosecute him in Milan.[331] But there has been no cooling of Italian-U.S. relations over the incident. In Germany, the government is investigating allegations that a German car salesman from the town of Ulm, traveling to Macedonia for a New Year's holiday was seized by Macedonian police at the border, held incommunicado for weeks without charge, then beaten, stripped, and flown to a jail in Afghanistan controlled by U.S. agents, where he was held and tortured for five months before being dumped in Albania.[332] Although German officials said they believed the man was innocent, no official protest had been lodged as of January 2005.

Meanwhile, as described earlier (see p. ???? above) there is evidence that the agencies of some Western liberal countries have actively cooperated with C.I.A. agents and security agencies in countries like Egypt and Tunisia, arranging for suspects to be picked up and interrogated or detained abroad by those agencies, and then sharing in the fruits of the interrogations.

Finally, it is clear that the governments of Austria, Canada, Germany, Sweden, Turkey, and the U.K. have themselves sought to deport terrorist suspects to countries where torture is a widespread or systemic problem, including

Egypt, Russia, the Philippines, Russia, Sri Lanka, Syria and Uzbekistan.[333]

h) New License for Brutal Regimes

At the same time, regimes whose human rights abuses have, in the past, elicited sharp criticism from Western liberal governments are now being tolerated, supported and even bolstered by those governments.

Since it launched its military campaign in Chechnya, Russia's leaders have characterized the armed conflict there as counter terrorism, glossing over the political aspects of it. But world leaders were critical of the gross human rights abuses of the Russian operation, which have included the indiscriminate bombing of civilian populations, village massacres, disappearances, mass arbitrary detentions, and torture. Weeks after the 9/11 attacks, however, democratic leaders like German Chancellor Gerhard Schroeder and Italy's Prime Minister Silvio Berlusconi were saying that they would have to judge Russian operations in Chechnya differently.[334]

In Egypt governments have ruled under an emergency law continously since 1981 and have routinely used their authority under the law to "arrest people at will and detain them without trial for prolonged periods, refer civilians to military or exceptional state security courts, and prohibit strikes, demonstrations, and public meetings". On the extension of the law in February 2003, a U.S. State Department spokesperson stated that the United States "under[stood] and appreciate[d] the Egyptian government's commitment to combat terrorism and maintain stability"[335]

In Georgia, where operations against Chechen rebels in the Pankisi Gorge have been brutal, involving extrajudicial execution, disappearances, arbitrary detention, and discrimination on the basis of racial and ethnic identity, the U.S. has established a $64 million "Train and Equip" program "to strengthen Georgia's counter-terrorism capability". At least six U.S. military personnel were present in Georgia as of October 2002 to provide training.[336] TIME magazine has reported that Georgian operatives have "disappeared" and killed suspects based on "real-time intelligence" provided by the U.S. Georgian officials have also admitted to the secret and extralegal rendition of individuals into U.S. custody.[337]

In Indonesia, the U.S. has renewed its links with the Indonesian military, which had been cut after the violence orchestrated by that military in East Timor in 1999. After September 11, 2001, the U.S. military training program was reinstated and a new $50 million program announced to assist Indonesian security forces in their counter terrorism efforts. In December 2002, a Kuwaiti citizen married to an Indonesian woman was arrested "and handed over to the U.S. authorities as part of an intelligence operation involving Indonesia's intelligence service and the C.I.A".[338]

In Malaysia, nearly 100 men have been held for alleged links to terrorist groups under the country's draconian *Internal Security Act* (*ISA*) – some for more than 3 years.[339] Prior to 9/11, the U.S. government had been extremely critical of the Malaysian government's detentions of opponents under the ISA and relations between the two countries were strained.[340] Since then, U.S. officials have praised the detentions[341] and President Bush has referred to the country as a "beacon of stability".[342] The U.S. has helped Malaysia to set up the Southeast Asia Regional Center for Counterterrorism and provided training there for Malaysian government officials.[343] "The Malaysian government regularly shares intelligence information with the U.S. government, and has offered the U.S. access to detainees in Malaysia. When the U.S. interrogated thirteen

Malaysian students detained without trial in Karachi, Pakistan, in September 2003, the Malaysian government remained silent rather than protest the detentions."[344]When the thirteen returned to Malaysia, the government detained them.[345] Detainees who have refused to cooperate with security officials in Malaysia have been told that they could be transferred to U.S. custody in Guantanamo Bay, Cuba.[346]

Former British ambassador to Uzbekistan, Craig Murray, has claimed that U.S. agents sent detainees from Afghanistan to that country to be interrogated using torture. Murray was removed from his post after sending a memo to the British Foreign Minister in which he reported that the C.I.A. station chief in Tashkent had "readily acknowledged torture was deployed [in Uzbekistan] in obtaining intelligence [from U.S. suspects]". [347] In Uzbekistan, Murray has stated, the "partial boiling of a hand or an arm is quite common [in interrogation]"[348] "I have seen post mortem photos of a corpse. These show that the person was boiled to death."[349]

In Latin America, the U.S. has intensified its support of the Colombian military in order to help it win a four decade old war against the leftist Revolutionary Army Forces of Colombia (FARC) and the National Liberation Army (ELN).[350] The head of the U.S. Southern Command told a Congressional panel in March 2004 that Washington "must take comprehensive measures in our region to combat terrorism" including, he said, strengthening Latin American militaries. He also suggested that Latin American countries should be encouraged to break down legal barriers between civilian policing, intelligence functions, and military functions.[351] Latin American militaries, in the past, have been responsible for some of the worst human rights abuses in the region.

Brutal or repressive regimes have been quick to point to the current practices of the U.S. to justify their own practices. The Liberian government claimed that an editor of one of Liberia's independent newspapers whom it had arrested could be held incommunicado and tried before a military court since he was an "illegal combatant" involved an Islamic fundamentalist war.**352** Egypt's President Mbarak has said "There is no doubt that the events of September 11 created a new concept of democracy that differs from the concept that Western states defended before these events, especially with regard to freedom of the individual." The U.S. decision to authorize the use of military tribunals in its "war on terror", he said, "proves that we were right from the beginning in using all means, including military tribunals."

THE ILLUSION OF SECURITY

Myth #9: These initiatives make us safer.

The global surveillance initiatives that governments have embarked upon do not make us more secure. They create only the illusion of security.

Sifting through an ocean of information with a net of bias and faulty logic, they yield outrageous numbers of false positives – and false negatives. The dragnet approach might make the public feel that something is being done, but the dragnet is easily circumvented by determined terrorists who are either not known to authorities, or who use identity theft to evade them.

For the statistically large number of people that will be wrongly identified or wrongly assessed as a risk under the system, the consequences can be dire.

At the same time, the democratic institutions and protections, which would be the safeguards

of individuals' personal security, are being weakened. And national sovereignty and the ability of national governments to protect citizens against the actions of other states (when they are willing) are being compromised as security functions become more and more deeply integrated.

The global surveillance dragnet diverts crucial resources and efforts away from the kind of investments that *would* make people safer. What is required is good information about specific threats, not crude racial profiling and useless information on the nearly 100 percent of the population that poses no threat whatsoever.

Good information about specific threats is usually obtained through human, not technological intelligence, by agents capable of infiltrating the circles where these threats exist. As security experts admitted in the aftermath of 9/11, these were the kind of critical resources that were lacking in U.S. security agencies at that time. There was a dearth of agents who possessed the background and languages relevant to the threat and a dearth of agents on the ground collecting human intelligence. Even translators were lacking. The Al Qaeda messages that were reportedly intercepted by the National Security Agency on September 10, 2001 ("Tomorrow is zero hour", "The match is about to begin") were not translated until days later. Three years after the attacks, more than 120,000 hours of recorded telephone calls had yet to be translated by the F.B.I.[353]

The global surveillance dragnet alienates the very communities from whom intelligence agencies need assistance, making it difficult to get crucial tips from them and difficult to recruit the law enforcement and intelligence officers needed from their ranks. The racial profiling that is endemic to the dragnet approach harasses and targets these communities wholesale. Ronald Noble, the black American who runs the 181-nation Interpol agency, says he himself has been singled out when travelling because of his looks:

> "I perspire and I'm the head on an international law enforcement agency …You have a lot of abuses that are never, ever checked."[354]

Global surveillance does nothing to address the root causes of terrorism – for example, poverty, dispossession, conflict, repressive governments and human rights abuses. The current security agenda treats the symptom instead of the disease. It proselytizes a skewed and narrow conception of human security, making terrorism – which by any measurement poses far less of a threat to human beings and to democracy than any of the above-listed threats – the preeminent focus.

In fact, the current security agenda *exacerbates* global insecurity. Its unjust targeting and stereotyping of Muslims, combined with the West's rhetoric about a clash of civilizations and its collusion with repressive regimes – and the brutal, lawless treatment meted out in the global gulag – engender hatred against Western countries and their partners, fomenting only more fanatical opposition and terrorism.

Myth #10: Guaranteeing security is the paramount responsibility of governments.

There is a widely held public opinion that governments should have known about and prevented the 9/11 plot. In fact, the traditional systems of intelligence and law enforcement that were in place at the time *did* yield information about the likelihood of an attack on U.S. soil by Muslim extremists using airplanes, and some of the key players in the 9/11 attacks were under investigation by the C.I.A. and F.B.I.

before the events.[355] The Joint Inquiry into the circumstances surrounding the 9/11 attacks conducted by the U.S. Senate and House intelligence committees reported that while the intelligence community did not have information on the "time, place and specific nature" of the 9/11 attacks, it had "amassed a great deal of valuable intelligence" that warned of the attacks.[356] The community's failure, according to the Joint Inquiry, was its inability

> …. to discern the bigger picture… to capitalize on both the individual and collective significance of available information…No one will ever know what might have happened had more connections been drawn between these disparate pieces of information …The important point is that the Intelligence Community, for a variety of reasons, did not bring together and fully appreciate a range of information that could have greatly enhanced its chances of uncovering and preventing Usama bin Ladin's plan to attack these United States on September 11, 2001.[357]

If U.S. agencies could not "see the forest for the trees" when they had specific information about a specific kind of threat and specific individuals, would it have helped them to have had to sift through information on the lives of hundreds of millions of people?

If there was failure in communication or analysis on the part of U.S. security agencies, there was also political failure on the part of the White House. While the Bush Administration refuses to reveal what it was briefed about and when prior to the attacks , sources indicate that it was briefed,[358] and the record shows that it took no steps to heighten security in appropriate areas. Under Attorney General John Ashcroft, the F.B.I.'s counter-terrorism program faced pressures for funding cuts. Despite the numerous intelligence warnings about the importance of the Al Qaeda threat, the C.I.A. unit focusing on bin Laden could not get the funding it needed. Lieut. General Michael Hayden, director of the National Security Agency (NSA), said that he knew in 2001 that the NSA needed to improve its coverage of Al Qaeda but that he was unable to obtain the resources for that effort.[359]

Neither bureaucratic failure nor the failure of political leadership would have been improved in any way by mass surveillance of the whole population. The 9/11 experience, itself, shows that authorities had enough trouble appreciating the significance of the specific, relevant information they did have. They did not need the ocean of general, irrelevant information they are now collecting, and very possibly they would have drowned in it altogether.

Myth #11: At least, these initiatives are better than doing nothing.

Careful examination shows that the global, mass registration and surveillance initiatives that have been described in this document are not "better than doing nothing". They divert resources away from activities that would provide us with better security, they are not effective, and the harm they do to democracies, individuals, the rule of law, and global security is not proportional to their utility, or even to the risk they are supposedly addressing.

It's time to tell our governments that they are on the wrong track, and to insist that they turn back from this dangerous road they are leading us down.

RESISTING THE REGISTRATION AND SURVEILLANCE AGENDA

The evidence and analysis in this report paints an alarming picture of a world that is not only

possible, but in the current political climate, probable. And, once the infrastructure that has been described is fully in place, it will be extremely difficult to dismantle it. These kinds of systems naturally accrete in the absence of sustained resistance. Corporate interests, advances in technology, function creep, and governments' need to prove that flawed systems only require more information in order to work, ensure accretion. If left unchecked, we could soon find ourselves living under regimes of all-pervasive surveillance.

This is not a global conspiracy, though there are certainly many agreements on the part of governments to act on different initiatives and a general intention among them to pursue the mass surveillance of populations. Rather, the surveillance agenda is fragmented across policy arenas and driven by a number of interests in each country, which include, as described earlier, domestic security, law enforcement, international relations, economic, class, and corporate interests.

To date, there has been relatively little resistance to the security/surveillance agenda on the part of civil society. The fragmentation of the agenda across policy arenas may be one explanation. However, the lack of resistance can also be explained by the fact that the issues are technical and multi-faceted, and government messaging about the need to provide security is powerful. Most media reports fail to "connect the dots" and paint the larger picture that would alert the public to what is going on. Measures are often presented as logical improvements on existing policing methods and, therefore, relatively benign. The critical decision-making that is being done by governments is regularly shielded from democratic scrutiny and public debate.

The development of global infrastructure surveillance for mass registration and surveillance, however, is by no means inevitable. This report is intended to serve as a wake-up call, and to inspire resistance and activism. To understand the world is to change it: all-pervasive surveillance can only become a reality if apathy and acquiescence prevail over concerns for human rights, civil liberties, and democratic standards. If and when public outrage reaches a critical mass, the initiatives and trends described in this report will be slowed and then stopped. This, however, cannot happen without widespread public awareness. Without public activism, we are in danger, as the U.K Privacy Commissioner has said, of "sleep-walking into surveillance societ[ies]".[360]

1. Pockets of Resistance

There are already pockets of resistance.

a) NGOs

Pressure from the Global Internet Liberty Campaign ("GILC") and others secured amendments to the draft Council of Europe *Convention on Cybercrime* and the deletion of its clauses on mandatory data retention; the GLIC continues to campaign on a host of issues.[361] The E.U. proposal for a binding Framework Decision on data retention was exposed by the E.U. group, Statewatch, in 2002 and a campaign from the European Digital Rights Initiative ("EDRi") saw the proposal removed from the E.U. agenda, if only temporarily. [362] The resurrection of the Framework Decision in 2004, in the wake of the Madrid bombings in March 2004, saw the U.K. group, Privacy International ("PI"), join EDRi in the campaign against a cross-Europe data retention regime, obtaining a compelling opinion from a London-based law firm which detailed how the proposal violated European human rights laws. PI also took the lead in crafting and circulating a joint statement calling on the European Commission to abandon

the proposal. [363] Those signing the statement ultimately included 80 European telecommunications companies and over 90 NGOs representing almost two dozen nations in Europe and elsewhere around the globe, though the proposal remains firmly on the table at the time of writing.[364]

There is also a developing campaign against the global surveillance of movement. PI, along with the American Civil Liberties Union (ACLU), Statewatch, EDRi and the Institute for Public Policy Research, for example, have been working together to oppose PNR sharing. They have written an open letter to ICAO and produced a detailed report on E.U.-U.S. negotiations for the transfer of European PNR.[365] The TransAtlantic Consumer Dialogue, a coalition of more than 60 consumer organizations in the U.S and Europe have passed a resolution calling on the E.U. and U.S. governments to suspend the sharing of PNR data until much stronger privacy safeguards are adopted.

There has also been growing resistance in national campaigns around the world to the proposed introduction of national ID cards, mandatory fingerprinting and biometric ID systems.[366]

The International Commission of Jurists and others have called on the U.N. to establish a mechanism within the U.N. system to monitor the effect of anti terrorism measures on human rights.[367]

Given that the U.S. is the catalyst and driver of the new security agenda around the world, resistance within the United States will be critical to stopping the agenda. Encouragingly, the U.S. is home to some of the most popular and successful resistance. The ACLU and other non-governmental organizations enjoy wide support in the U.S. in their work against domestic policies and they are fighting on many fronts. The ACLU, for example, has started a campaign calling on consumers to pressure corporations regarding the protection of personal information.[368] It has also mounted sustained opposition to the Total Information Awareness program and successor programs in the U.S.[369] It has been fighting MATRIX,[370] CAPPS II[371] and working to discover how the U.S. government's secret watch lists operate.[372] It has researched and exposed government and private sector synergies in the area of surveillance.[373]

b) Democratic Institutions

Although, to date, much of the resistance and analysis has come from NGOs with mandates dedicated to privacy and civil liberties, their concerns are beginning to reverberate in democratic institutions.

Data Protection and Privacy Commissioners, for example, have protested incursions made by the "war on terror" on privacy protections *en bloc*, attempting to alert the rest of society to the broader dangers ahead, once privacy is violated. E.U. Data Protection Commissioners have opposed successive E.U. proposals and agreements on data retention, on the exchange of passenger data with the U.S., and on the creation of a biometric population database. At the International Conference of Data Protection and Privacy Commissioners in Australia, in September 2003, participants warned that the "war on terror" is in "danger of undermining democracy and freedom by measures designed to defend it".[374] More recently, the Czech Data Protection Officer reminded the public that:

> *"Privacy is one of the basic values of human life and personal data is the main gateway enabling entry into it. The citizens of countries that experienced a period of totalitarian regimes have that hard experience – when privacy was not considered of value and was sacrificed to the interest of the state"* [375]

Concerns about the surveillance agenda are also filtering into democratic bodies. Multi party committees in houses of government around the world are taking a critical view of the measures that are being brought before them, and often acting to defeat or at least delay implementation. In Canada, the *Public Safety Act* was tabled three times with amendments before being passed. In the U.S. there has been greater scrutiny by Congress of legislation augmenting the *USA_PATRIOT ACT* (known as *PATRIOT ACT* II) than there was of the original act. As mentioned earlier in this report, the U.S. General Accounting Office has produced reports that have detailed and criticized CAPPS II and the data mining projects of the U.S. government.[376] The CAPPS II report led to the withdrawal of the program. The Office of the Inspector General has produced a report that criticized government treatment of detainees held on immigration charges.[377] In the U.K., there was outspoken opposition in the House of Commons from members of all parties about the proposal to introduce a U.K. national ID card. In Europe, as described earlier, the European Parliament has vigorously objected to the deal struck by the E.U. Commission to share E.U. PNR with the U.S.

In a few cases, governments themselves have acted to protest or roll back laws. In the U.S., more than 370 local authorities in 41 states have passed resolutions opposing parts of the *USA PATRIOT ACT*.[378] Brazil has imposed the same fingerprinting on American travelers at its borders that the U.S. imposes on Brazilian citizens under the U.S.-VISIT program. The new government in India has repealed India's *Prevention of Terrorism Act* (*POTA)*, adopted in haste in December 2001. Citing the fact that *POTA* had been used to justify gross human rights violations, particularly against Muslims from Kashmir and Gujurat, the new government said it would continue to combat terrorism but with laws existing before September 2001.[379]

Some governments have taken action under political pressure. After sustained public pressure and criticism from the mainstream media, the Canadian government agreed to hold a public inquiry into Canada's role in Maher Arar's rendition from the U.S. to Syria. However, government authorities are doing their best to limit scrutiny of their actions, as American and British officials also have in the various inquiries into intelligence on Iraq, the handling of intelligence leading up to September 11, and the death of British scientist, Dr. David Kelly.

c) Courts

The courts in a number of countries have struck down or ruled against a number of antiterrorism measures.

The House of Lords recently ruled (7 to 1) that the detention of foreigners without charge taking place under the U.K. *Anti-Terrorism Act* were discriminatory and violated European human rights standards against arbitrary detention and discrimination.[380] Lord Nichols of Birkenhead wrote that "[i]ndefinite imprisonment without charge or trial is anathema in any country which observes the rule of law."[381] Lord Hoffman rejected the government's contention that a derogation from the prohibition on arbitrary detention was justified on the basis of a "threat to the life of the nation". "Terrorist violence", he wrote, "serious as it is, does not threaten our institutions of government or our existence as a civil community… The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from [draconian] laws."[382]

In *Rasul v. Bush*, the U.S. Supreme Court held importantly that "the federal courts have jurisdiction to determine the legality of the Executive's potentially indefinite detention of individuals who claim to be wholly innocent wrongdoing."[383] In *Hamdi v. Rumsfeld* the

Supreme Court wrote, "a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens". The court majority held that Hamdi, a U.S. citizen allegedly captured on the battlefield in Afghanistan, and held incommunicado for more than two years on various military brigs without charges and trial, had a right to know the factual basis for his "enemy combatant" classification, and to rebut these assertions of fact before a neutral decision-maker. In *Rumsfeld v. Padilla*, a petition for *habeas corpus* made by a U.S. citizen arrested and detained in the U.S. was dismissed by the Supreme Court on the basis that it had been filed in the wrong court. In the new claim, the Federal District Court ruled in March 2005 that

> "the president has no power, neither express nor implied, neither constitutional nor statutory, to hold petitioner as an enemy combatant"[384]

A recent District Court decision has also found that the special trials established by the government following the Supreme Court's decision in *Rasul v. Bush* and *Hamdi v. Runsfeld*, to determine the guilt or innocence of detainees in Guantanomo Bay, were unlawful and could not continue in their current form since the detainees may be "prisoners of war" and therefore entitled to a higher standard of justice under the *Geneva Conventions*.[385] Finally, in *Doe and ACLU v. Ashcroft et al*., the Federal District Court struck down a provision in the *USA PATRIOT ACT* that gave the government unchecked authority to issue "National Security Letters to obtain sensitive customer records from Internet service providers and other businesses without judicial oversight. The court also found a broad 'gag' clause in the provision to be an unconstitutional 'prior restraint' on free speech, saying 'democracy abhors undue secrecy'".[386]

Courts in other countries have similarly struck down anti terrorism laws passed since September 11, 2001.[387] In Indonesia, a top court has ruled that that the tough anti terrorism law No. 16 used to convict the Bali bombers was unconstitutional.[388] In Austria, the Federal Constitutional Court has held that a statute compelling telecommunication service providers to implement wiretapping measures at their own expense is unconstitutional.[389] Finally, in Germany, the Constitutional Court recently declared portions of a law for telecommunication interception unconstitutional because it violated the communications secrecy guaranteed in art. 10 of the German constitution. This ruling may have implications for data retention in Germany.[390]

2. The Future is in Our Hands

The *Universal Declaration of Human Rights* is one of the seminal documents of the post World War II order, enshrining a collective commitment to a new world in which the dignity of all persons was to respected and acknowledged as the inalienable birthright of mankind. Its contents have been incorporated into constitutions and treaties around the world, becoming in the process, international customary law.

But if the *Universal Declaration* ushered in an age of human rights, the disregard that governments around the world are now showing for its principles may be the ominous portent of that age's demise. Certainly, its rights-based protections for individuals are the antithesis of the current risk-based paradigm which governments are now espousing.

This report has identified infringements of no less than half of the minimum standards contained in the *Declaration*. In addition to the right to privacy (art. 12), these include the ban on racial discrimination (art. 2), the right to liberty and security of person (art. 3), the prohibi-

tion of torture, inhumane and degrading treatment (art. 5), the right to recognition and equality before the law (arts. 6 and 7), the right to an effective legal remedy (art. 8), the prohibition on arbitrary arrest, detention or exile (art. 9), the right to a fair and public hearing by an independent and impartial tribunal (art. 10), the presumption of innocence (art. 11), the right to freedom of movement (art. 13), the right to freedom of thought, conscience and religion (art. 18), freedom of expression (art. 19), freedom of peaceful assembly and association (art. 20), and the entitlement to a social and international order in which rights and freedoms can be fully realized (art. 28).

If human rights and civil liberties are to survive into the 21st century, there must be a sea change in political and popular culture. The resistance that has occurred to date is not enough. Groups and individuals across the whole spectrum of civil society must play a part. The future is in all of our hands.

Endnotes

Note: Dates in square brackets after on-line addresses refer to the most recent dates the websites or on-line documents were accessed.

[1] Reg Whitaker, *The End of Privacy* (New York: The New Press, 1999), p. 25. [*Reg Whitaker*]

[2] Reg Whitaker, *TIbid.he End of Privacy*, p. 45.

[3] Reg Whitaker, *ThIbid.e End of Privacy*, p. 45.

[4] Estanislao Oziewicz, "Shroud lifting on global gulag set up to fight 'war on terror'", *The Globe & Mail,* May 13, 2004, page A14. [*Estanislao Oziewicz*]

[5] Thomas Mathiesen, *On Globalistion of Control: Towards an Integrated Surveillance System in E.U.rope* (London: Instant Print West, November 1999), p. 3. Available from Statewatch (http://www.statewatch. org, or e-mail office@statewatch.org). [*Thomas Mathiesen*]

[6] "Once the Belgians had decided to limit administrative posts and higher education to the Tutsi, they were faced with the challenge of deciding exactly who was Tutsi. Physical characteristics identified some, but not for all. Because group affiliation was supposedly inherited, genealogy provided the best guide to a person's status, but tracing genealogies was time-consuming and could also be inaccurate, given that individuals could change category as their fortunes rose or fell. The Belgians decided that the most efficient procedure was simply to register everyone, noting their group affiliation in writing, once and for all. All Rwandans born subsequently would also be registered as Tutsi, Hutu, or Twa at the time of their birth. The system was put into effect in the 1930s. Human Rights Watch, *Leave None to Tell the Story: Genocide in Rwanda,* April 1, 2004.http://www.hrw.org/reports/1999/rwanda/Geno1-3-09.htm [March 5, 2005].

[7] See Office of the Inspector General, United States Department of Justice, *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks*, June 2003. http://www.usdoj.gov/oig/special/0306/index.htm [December 30, 2004]. [*Office of the Inspector General Report on Detainees*].

[8] Federal Register, Final Rule dated August 12, 2002; 8 CFR 264. See also, National Security Entry-Exit Registration (NSEERS) Summary Chart, February 25, 2003. http://64.233.167.104/search?q=cache:-34s3QXmzLMJ:www.oiss.wayne.edu/Forms/PDF/NSEERS_SUMMARY_CHART.pdf+NSEERS&hl=en [March 5., 2005].

[9] Asian American Legal Defense and Education Fund (AALDEF), *Special Registration: Discrimination and Xenophobia as Government Policy* (AALDEF,, 2004), p. 1. http://www.aaldef.org/images/01-04_registration.pdf [November 24, 2004].

[10] *Ibid.*

[11] Immigration Policy Center, "Targets of Suspicion: The Impact of Post-9/11 Policies on Muslims, Arabs and South Asians in the United States", *Immigration Policy In Focus*, Vol. 3, Issue 2 (May 2004) p. 7. http://www.ailf.org/ipc/ipf051704.pdf [December 1, 2004]. See also, Flynn McRoberts, "Muslim exodus from U.S. unravels tight knit enclaves", *Chicago Tribune*, November 18, 2003.

[12] The US-VISIT program requirements apply to all visitors except (as of December 2004) Mexican citizens holding "border crossing cards" or "laser visas" and most Canadian citizens. See U.S. Department of Homeland Security, *US-VISIT Fact Sheet: U.S.-Canada Land Borders*, and *US-VISIT Fact Sheet: U.S.-Mexico Land Borders.*, available online at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0435.xml [December 30, 2004].

[13] Associated Press, "U.S. eye scan plan under scrutiny: U.S. demanding biometric technology in passports; world may not be ready", *The Okanogan,* August 24, 2003.

[14] See, Statewatch, "Biometrics – the E.U. takes another step down the road to 1984", *Statewatch News Online,* September 2003. http://www.statewatch.org/news/2003/sep/19E.U.biometric.htm [March 5, 2005]; E.U.ractive, News, February 7, 2005. http://www.E.U.euractiv.com/Article?tcmuri=tcm:29-133939-16&type=News. [February 7, 2005].

[15] Lynda Hurst, "Bio-Security Still a Fantasy; Airport Screening Won't Work: Experts; No information to identify terrorists", *The Toronto Star*, January 24, 2004, p. A1. [*Lynda Hurst*]

[16] Ryan Singel, "CAPPS II stands alone, feds say", *Wired News*, January 13, 2004. http://www.wired.com/news/privacy/0,1848,61891,00.html?tw=wn_story_related [March 6, 2005]. [*Ryan Singel*]

[17] Eric Lichtblau and John Markoff, "U.S. Nearing Deal on Way to Track Foreign Visitors", *New York Times*, May 24, 2004. http://travel2.nytimes.com/mem/travel/article-page.html?res=9903EEDD173EF937A15756C0A9629C8B63 [December 23, 2004]. [*Lichtblau and Markoff*]. GET key cite ?BORDC?that says foreign and commercial databases

[18] The Federal Register Notice states that "[i]t is . . . anticipated that CAPPS II will be linked with the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program at such time as both programs become fully operational, in order that processes at both border and airport points of entry and exit are consistent." See also, Questions Submitted for the Record by Senator Ron Wyden, Oversight Hearing for Transportation Security, September 9, 2003.

http://www.eff.org/Privacy/cappsii/20030909_wyden_questions.php [March 6, 2005]. "U.S. officials said they are considering merging the two programs [U.S. VISIT and CAPPS II]." Sara Kehaulani Goo, "U.S. to Push for Passenger Records: Travel Database to Rate Security Risk Factors, *Washington Post*, January 12, 2004, p. A01; and Interim Final Rule and Notice, 69 Federal Register 467 (January 5, 2004). http://a257.g.akamaitech.net/7/257/2422/05jan20040800/edocket.access.gpo.gov/2004/pdf/03-32331.pdf [January, 2005]. The rule "requires the integration of all databases that process or contain information on aliens". Compare, Ryan Singel, *supra* note 16.

[19] Lynda Hurst, *supra* note 15. See also, ACLU, "ACLU Criticizes Plans to Go Forward with CAPPS II, Calls Dragnet Profiling Approach Fake Security on the Cheap", Media Release, January 12, 2004. http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=14699&c=206 [March 4, 2005]. The term "black box" is also used to refer to Internet monitoring devices on ISP networks to monitor user traffic. Little is publicly known about the workings of these, except that they are like the "'packet sniffers' typically employed by computer network operators for security and maintenance purposes. Packet sniffers are specialized software programs running in a computer that is hooked into the network at a location where it can monitor traffic flowing in and out of systems. Sniffers can monitor the entire data stream searching for key words, phrases or strings such as net addresses or e-mail accounts. They can then record or retransmit for further review anything that fits their search criteria. Black boxes are apparently connected directly to government agencies by high speed links in some countries. Privacy International, *Privacy and Human Rights 2003, Executive Summary*. http://www.privacyinternational.org/survey/phr2003/threats.htm [March 5, 2005, 2005].

[20] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, PL 107-56, s. 215 (Washington: GPO, 2001). http://thomas.loc.gov [November 25, 2004].

[21] Due to public concerns expressed about privacy, the Lockheed Martin group was eventually only awarded a contract to assist in the census by providing advanced systems and processing technologies. Statistics Canada, "Role of private contractors in the census", n.d. http://www12.statcan.ca/english/census06/info/outsource/outsourcing.cfm [December 20, 2004].

[22] See British Columbia Ministry of Health Services, "Government Moves to Improve MSP and Pharmacare Services", News Release, November 4, 2004: and "Backgrounder: Maximus BC/Alternative Service Delivery", both available on-line at http://www.healthservices.gov.bc.ca/msp/ [December 20, 2004].

[23] B.C. Hydro, "B.C. Hydro and Accenture Agreement Designed to Save $250 Million in Costs", News Release, February 28, 2003. http://www.bchydro.com/news/2003/feb/release4622.html [December 20, 2004].

[24] Steven Donziger, "The Twilight-Zone Court, *The Nation*, September 22, 2003.

[25] See Patrick Healy, "Colleges giving probers data on foreign students' finances", *Boston Globe*, Oct. 3, 2001. American Association of Collegiate Registrars and Admissions Officers, "Preliminary Results of the AACRAO Survey on Campus Consequences of the September 11 Attacks", October 4, 2001. http://www.aacrao.org/transcript/index.cfm [December 19, 2004].

[26] Stephanie Stoughton, "Poll: Firms Relaxed Privacy Rules", *Boston Globe*, October 8, 2001.

[27] Eunice Moscoso, "Demand for data by feds on rise", Cox Washington Bureau, August 17, 2003. http://www.federalobserver.com/print.php?aid=6378 [December 18, 2004].

[28] See the website of InfraGard: Guarding the Nation's Infrastructure, http://www.infragard.net [November 24, 2004]. As of November 22, 2004, the number of InfraGard members was given as 14,536.

[29] Chris Seper, "Combating Cybercrime: FBI's InfraGard Program Promotes Security Awareness", *Cleveland Plain Dealer*, Nov. 4, 2002. http://www.infragard.net [November 24, 2004].

[30] Ryan Singel, "JetBlue Shared Passenger Data", *Wired News*, September 18, 2003; Ryan Singel and Noah Schachtman, "Army Admits to Using JetBlue Data", *Wired News*, September 23, 2003. http://www.wired.com/news/privacy [November 24, 2004].

[31] Electronic Privacy Information Center, "Northwest Airlines gave NASA Personal Info on Millions of Passengers; Disclosure Violated Privacy Policy", Press release, Jan. 18, 2004. http://www.epic.org/privacy/airtravel/nasa/pr1.18.04.html [November 24, 2004]. See also: Sara Kehaulani Goo, "Northwest Gave U.S. Data on Passengers", *Washington Post*, January 18, 2004. http://www.washingtonpost.com/wp-dyn/articles/A26422-2004Jan17.html [November 24, 2004].

[32] Sara Kehaulani Goo, "American Airlines Revealed Passenger Data", *The Washington Post*, April 10, 2004, p. D12. http://www.washingtonpost.com/wp-dyn/articles/A720-2004Apr9.html [December 7, 2004].

[33] John Schwartz and Micheline Maynard, "FBI got Records on Air Travelers*", New York Times*, May 1, 2004.

[34] DoubleClick, "Abacus B2C Alliance",

http://www.doubleclick.com/us/products/direct_marketing/abacus_b2C_alliance/ [December 21, 2004].

[35] Jim Krane (Associated Press), "Information bank reaches into Latin America: U.S. buys access to personal data", *Daily News (Los Angeles)*, April 20, 2003. http://portal-pfc.org/english/articles/2003/039.html [December 21, 2004]. According to

ACLU researchers, no country in Latin America has protections in place against the export of data.

[36] *Ibid.*

[37] In the novel *Brave New World*, a totalitarian government controls society through the use of science and technology. Aldous Huxley, *Brave New World,* 1932, 1946 (New York: Harper Collins, 1998).

[38] "Smart cards make inroads into Asia", *Asian Times*, October 2004. *["Smart cards make inroads in Asia"*]

[39] House of Commons Canada, Interim Report of the Standing Committee on Citizenship and Immigration, *A National Identity Card for Canada?*, October 2003, pp. 16-23. [*A National Identity Card for Canada?*] http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06-e.htm [November 24, 2004].

[40] Initially, the U.S. exempted 28 visa waiver countries from the requirements of the U.S. VISIT program provided they implemented biometric passports by an October 2004 deadline. However, when it became clear that countries were not going to be able to meet the deadline, the U.S. VISIT program was extended to all countries with the exception of Canada, which enjoys a partial exemption in respect of Canadian citizens travelling to the U.S. without work or student visas. Once visa waiver countries implement machine readable biometric passports, fingerprinting of their nationals under the U.S. VISIT program may stop, but it may also continue if the passports adopted do not incorporate a fingerprint biometric. See http://news.bbc.co.uk/2/hi/americas/3595221.htm [November 2004]; Tim Harper, "U.S. to Screen Canadians", *The Toronto Star*, January 6, 2004.

[41] See Statewatch, "E.U. Summit: Agreement on "harmonised" biometric identification linked to E.U. databases", *Statewatch News online*, June 2003. http://www.statewatch.org/news/2003/jun/22bio.htm [December 13, 2004].

[42] At the outset of its deliberations, ICAO promised to design standards that upheld national data protection laws and cultural practices in the domestic and transborder use of information, but it did none of this. See Open Letter to ICAO, March 30, 2004. www.privacyinternational.org/ issues/terrorism/rpt/icao-letter.pdf [March 5, 2005].

[43] On December 13, 2004, the E.U. General Affairs Council adopted a regulation on mandatory facial images and fingerprints in E.U. passports. See Euractive, "Newly issued passports to include fingerprints", December 15, 2004. http://www.euractiv.com/Article?tcmuri=tcm:29-133440-16&type=ShortNews [March 5, 2004].

[44] International Civil Aviation Organization, "Biometric Technology in Machine Readable Travel Documents – The ICAO Blueprint", FAL-12-WP/4, 5/11/03, Presented to the Twelfth Meeting of the Facilitation Division of the International Civil Aviation Organization, March 22-April 2, 2004, Cairo, Egypt. http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp004_en.pdf [December 3, 2004].

[45] See *A National Identity Card for Canada?*, *supra* note 39.

[46] With the release of the Commons Committee report in early October, Citizenship Minister Denis Coderre was immediately put on the defensive. See, for example, Tyler Hamilton, "Security-as-Theatre, Intrusive, Ineffective Smoke and Mirrors Security Fails" *The Toronto Star*, September 1, 2003, p. D1. [*Tyler Hamilton*] At a public forum on national ID cards organized by Coderre's Ministry and held on October 7 and 8, 2003, civil society groups and privacy commissioners criticized Coderre's proposal to introduce a national ID card, and also the heavy participation of industry in the forum.

[47] The Canadian Press, "Ottawa to introduce biometric passports", *The Toronto Star*, July 18, 2004.

[48] *Ibid.*

[49] The U.S. Congress set October 26, 2004 as the deadline by which both U.S. and foreign passports were to be upgraded to include biometric identification, but the U.S. along with other countries were unable to meet the deadline. See, "Iris-recognition will become common at border crossings into the United States by the end of the year", *National Post*, August 28, 2004, p. FP7; Tyler Hamilton, *supra* note 46.

[50] Kamal Ahmed, "Ministers to dump 'useless' identity card", *The Observer*, October 12, 2003.

[51] At the G8 meeting, the U.K. Home Secretary said that biometric data would be included in U.K passports from 2006. Kristina Merkner and Elise Kissling, "Germany to shape E.U. passport rules", *Frankfurter Allgemeine Zeitung (F.A.Z.)*, June 27, 2003.

[52] Tanya Branigan, "Lords could sink ID Bill admits Clarke", *The Guardian,* February 11, 2005. http://www.guardian.co.uk/idcards/story/ 0,15642,1410578,00.html [March 6, 2005].

[53] BBC News, "Concern over biometric passports", March 30, 2004. http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/technology/3582461.stm [April 22, 2004].

[54] Government of the United States, "Face Recognition for Identity Confirmation – Inspection of Travel Documents", FAL/12-WP/63, 10/3/04, Presented to the Twelfth Meeting of the Facilitation Division of the International Civil Aviation Organization, March 22-April 2, 2004, Cairo, Egypt. http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp063_en.pdf

[November 25, 2004].

[55] Lynda Hurst, *supra* note15*,* p. A1.

[56] David Colker and Joseph Menn, "Choicepoint CEO had Denied any Earlier Breach of Database", *Los Angeles Times,* March 3, 2005. http://www.newsday.com/business/la-fi-choicepoint3mar03,0,6289300.story?coll=ny-business-headlines [March 6, 2005].

[57] Lynda Hurst, *supra* note 15, p. A1.

[58] See, for example, Government of Canada, "The Canadian Advance Passenger Information Program", FAL/12-WP/38,11/12/03, Presented to the Twelfth Meeting of the Facilitation Division of the International Civil Aviation Organization, March 22-April 2, 2004, Cairo, Egypt, point 1.3. http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp038_en.pdf [November 25, 2004] [*Canadian Submission on PNR to ICAO)*]; Tonda MacCharles, "Air travellers face screening; Canadian program aims at terrorist 'risk scoring' system; Information would be shared with U.S., documents show", *Toronto Star*, January 17. 2004. [*Tonda McCharles*].

[59] Privacy International, *First Report on Towards an International Infrastructure for Surveillance of Movement: Transferring Privacy: the Transfer of Passenger Records and the Abdication of Privacy Protection*, February 2004, p. 2. [*Transferring Privacy*]

[60] See, for example, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal L 281,* 23/11/1995, pp. 0031-0050. http://europa.eu.int/comm/internal_market/privacy/law_en.htm [December 13, 2004]; and the Canadian *Personal Information Protection and Electronic Documents Act,* 2000. http://www.privcom.gc.ca/legislation/02_06_01_e.asp [November 25, 2004]. *Habeas corpus* laws in Latin America contain similar principles.

[61] *The Smart Border Declaration*, December 12, 2001. http://www.dfait-maeci.gc.ca/can-am/menu-en.asp?act=v&mid=1&cat=10&did=1669 [November 30, 2004]. *Action Plan for Creating a Secure and Smart Border*, http://www.dfait-maeci.gc.ca/can-am/menu-en.asp?act=v&mid=1&cat=10&did=1670 [November 30, 2004].[*Smart Border Action Plan*]

[62] *An Act to amend the Aeronautics Act*, 2001, c. 38, s. 1. http://laws.just. ice.gc.ca/en/2001/38/text.html [November 25, 2004].

[63] *Transferring Privacy*, *supra* note 59, p. i.

[64] "E.U.-US PNR: Council to ignore parliament and go ahead with "deal", *Statewatch News Online*, April 2004. http://www.statewatch.org/news/2004/apr/13ep-vote-pnr-court.htm. [March 2005]. [*Council to ignore parliament*]

[65] "All the national authorities competent for data protection in Europe have declared these transfers incompatible with European privacy laws." Letter from Graham Watson MEP, Enrique Baron Crispo MEP, and Johanna Boogerd-Quaak MEP, rapporteur, to fellow Members of the European Parliament, dated April, 2004 [*MEP letter*]. See also *Transferring Privacy*, *supra* note 59, p. 2.

[66] *Transferring Privacy*, *supra* note 59, p. 5.

[67] MEP letter, *supra* note 65.

[68] *Ibid.*

[69] In the current agreement, the retention period is 3.5 years. *Transferring Privacy*, *supra* note 59, p. 11.

[70] *Transferring Privacy*, *supra* note 53, p. 10.

[71] [*Council to ignore parliament*], *supra* note 64.

[72] Ian Black, "E.U. hands over data on air travelers", *The Guardian*, May 18, 2004.

[73] See *Transferring Privacy*, *supra* note 59, pp. 5-9; and Privacy International, "Report on Transfers of Air Passenger Data to the U.S. Department of Homeland Security", Media Release, February 2, 2004.

[74] See Statewatch, Observatory on E.U. PNR Scheme. http://www.statewatch.org./eu-pnrobservatory.htm [March 2005].

[75] "In September 2003, the Commission decided to accelerate work on developing an international arrangement for PNR data transfers within ICAO. The Commission services have prepared a working paper to this effect that will be submitted by the Community and its Member States to ICAO shortly." Commission of the European Communities, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE PARLIAMENT: *Transfer of Air Passenger Name Record (PNR) Data: A Global E.U. Approach,* Brussels: European Union, 2003,COM(2003) 826 final, December 16. European Community and its Member States, "An International Framework for the Transfer of Passenger Name Record (PNR) Data", FAL/12-WP/75, 15/3/04, Presented to the Twelfth Meeting of the Facilitation Division of the International Civil Aviation Organization, March 22-April 2, 2004, Cairo, Egypt. http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp075_en.pdf [November 25, 2004]. [*E.U. submission to ICAO*]

[76] *Ibid.*, point 1.1.

[77] Canadian Submission on PNR to ICAO, *supra* note 58*,* point 1.3. See also, Beth Gorham, "Domestic Passengers to be screened: Ottawa looking at kinds of information that can be collected", *The Vancouver Sun*, January 31, 2004, p. A9, reporting plans to expand the Canada Customs and Revenue Agency database on air passengers on incoming international flights to passengers arriving by bus, boat and train.

[78] Under the Canadian *Public Safety Act*.

[79] Spokeperson Suzanne Luber, said the new program replacing the Computer Assisted Passenger Prescreening Systems (CAPPS II) will cover all passengers traveling to and from the United States and within the country. Tim Harper, "U.S. ditches travel surveillance plan", *The Toronto Star*, July 16, 2004.

[80] David Blunkett, U.K. Home Secretary, has pushed a biometric identifier for every individual in the U.K. that would be linked to a national database, by saying it would allow the British "the freedom to do easily things like travel to Florida on holiday." But, of course, they could travel to Florida easily before. Statewatch, "*UK: "The Government intends to introduce a national compulsory ID cards scheme using an individual biometric identifier linked to a new national database" Statewatch News Online,* April 2004. http://www.statewatch.org/news/2004/apr/18uk-id-cards.htm [December 21, 2004].

[81] John Lettice, "Got a ticket? Get a record. E.U.-US data handover deal leaks", *The Register*, February 3, 2004. http://www.theregister.co.uk/2004/02/03/got_a_ticket_get/ [December 21, 2004].

[82] Three examples of such legislation are the *USA PATRIOT ACT*, the Colombian *Anti-terrorism Act*, and the Canadian *Anti-terrorism Act*.

[83] American Civil Liberties Union, *The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*, written by Jay Stanley (New York: ACLU, 2004), p. 14. http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16226&c=207 [November 22, 2004]. [*ACLU, The Surveillance Industrial Complex*]

[84] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 14.

[85] Kevin Poulsen*,* "War of Words Rages over Internet Taps", *Security Focus*, April 14, 2004. http://www.securityfocus.com/news/8454 [November 25, 2004]. [*Kevin Poulsen*]

[86] United States, *The National Strategy to Secure Cyberspace,* February 2003. http://www.whitehouse.gov/pcipb/ [November 25, 2004].

[87] These included Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Turkey, Ukraine and the United Kingdom.

[88] Council of Europe, *Convention on Cybercrime* (Budapest: 2001), arts. 20 and 21. See also art.1 definitions of "computer system" and "service provider". http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [November 25, 2004]. [*Convention on Cybercrime*]

[89] *Ibid.,* arts. 16, 20 and 21.

[90] *Ibid.,* arts. 16 and 17.

[91] *Ibid.,* arts. 25(4) and (5), and 27.

[92] See Kevin Poulsen, *supra* note 86 for a description of what is happening in the U.S. In Canada, the federal government released a consultation document on "lawful access" in 2002 which suggested that service providers would have to build surveillance capacity into their systems. Department of Justice, Industry Canada and Solicitor General Canada, "Lawful Access – Consultation Document", August 25, 2002. http://www.canada.justice.gc.ca/en/cons/la_al/consultation_index.html [November 25, 2004]. The Canadian government is planning to table lawful access legislation in 2005.

[93] See "Memorandum of Understanding concerning the lawful interception of telecommunications", ENFOPOL 112, 10037/95, Limite, Brussels, 25.11.95.

[94] *Convention on Cybercrime*, *supra* note 88.

[95] See Privacy International, "Privacy and Human Rights 2003, Executive Summary", pps. 18 and 19. http://www.privacyinternational.org/survey/ phr2003/threats.htm [March 5, 2005].

[96] Originating from a G8 ministerial sub-group.

[97] This was among more than 40 demands. See Statewatch, "Text of U.S. Letter from Bush with Demands for E.U. for Cooperation", *Statewatch News Online*. http://www.statewatch.org/news/2001/nov/06uslet.htm [March 5, 2005].

[98] See Statewatch, "Data retention comes to roost – telephone and internet privacy to be abolished", *Statewatch News Online.* http://www.statewatch.org/news/2004/apr/21dataretention.htm [March 5, 2005]. See also, "E.U.: data retention to be 'compulsory' for 12-24 months", *Statewatch News Online.* http://www.statewatch.org/news/aug/o5datafd1.htm [February 2005].

[99] David Akin, "Arrests key win for NSA hackers", *The Globe & Mail*, April 6, 2004.

[100] ECHELON is a secret program but information about it has been exposed in a 1996 book by Nicky Hager, called *Secret Power: New Zealand's role in the International Spy Network* (Nelson, New Zealand: Craig Potton Publishing, 1996). See also European Parliament, *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) 2001/2098(INI),* Final A5-0264/2001 PAR 1, July 11, 2001. http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_en.pdf [December 13, 2004].

[101] United Nations Security Council, *Resolution 1373 (2001),*

S/RES/1373 (2001). http://www.un.org/Docs/sc/committees/1373/resolutions.html [December 9, 2004].

[102] The U.S. Money Laundering Strategy of 2003 deals extensively with terrorist financing. See http://www.treas.gov/offices/enforcement/publications/ ml2003.pdf. One of the 'Six Key Objectives' of the Strategy is "establishing and promoting international standards to be adopted by countries" and "ensuring that countries throughout the world consistently implement these international standards". See further, the work of the Financial Action Task Force (FATF), the Egmont Group of Financial Intelligence Units, the G-20 and the International Financial Institutions, all of which provided a framework for combating money laundering before 9/11. This framework has been expanded to address terrorist financing and envisages sanctions for non-cooperating states.

[103] See http://europa.eu.int/comm/external_relations/un/docs/eu1373.pdf [March 5, 2005]

[104] Unless otherwise noted, dollar figures in this document are in U.S. dollars.

[105] *USA PATRIOT ACT, supra* note 20, s. 365.

[106] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 18.

[107] See further, 2002 FATF guidelines entitled "International Best Practices for Combating the Abuse of Non-Profit Organizations". http://www1.oecd.org/fatf/pdf/SR8-NPO_en.pdf. [February 2005]. See also, Statewatch "Charities and NGOs targeted in "war on terror", *Statewatch News Online*, January 2005.http://www.statewatch.org/news/2005/jan/08charities.htm [February 2005].

[108] The Schengen Information System contains records on people wanted by the police or judicial authorities, people to be refused entry at external borders (mainly rejected asylum applicants and people subject to deportation orders), people to be placed under surveillance, and on stolen vehicles, documents, works of art and other objects. As of 2004, there are already some 15 million records in the SIS and 125,000 access points.

[109] Sources for MATRIX include records on property ownership, FAA pilot licenses and aircraft ownership, Coast Guard registered vessels, sexual offenders lists, federal terrorist watch lists, corporation filings, bankruptcy filings, Uniform Commercial Code filings, and professional licenses. See Associated Press, "Early database project yielded 120,000 suspects; Scoring system cited for Matrix project spurs privacy worries", May 21, 2004. http://www.cnn.com/2004/LAW/05/20/terror.database.ap/ [November 25, 2004].

[110] Seisint Inc., "Matrix Michigan Briefing", May 8, 2003, slide entitled "Seisint's Core Capabilities" (document obtained through open records request filed by ACLU), cited in ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 24.

[111] Jim Bronskill, "Canada's justice supercomputer plan hits snag", *The Globe & Mail*, April 19, 2004.

[112] Statewatch, "Proposed exchange of personal data between Europol and U.S.A. evades E.U. data protection rights and protections", *Statewatch News Online*, November 2002. http://www.statewatch.org/news/2002/nov/12eurousa.htm [December 13, 2004].

[113] Statewatch, "E.U.: Council capitulates and releases draft E.U.-US agreements", *Statewatch News Online*. http://www.statewatch.org/news/2003/may/06useu.htm. [February 2005]. On January 3, 2005 *The Guardian* newspaper reported that two organisations in the U.K. set up to help the Palestinian people had their bank accounts abruptly closed without explanation. Both groups claimed their targeting was political. The Palestine Solidarity Campaign, a long established group, had its account closed by the Alliance & Leicester Bank in July 2004. Zoe Mars, the treasurer for the PSC, said that at the end of 2003 the group sent £750 to a medical charity in Palestine. Five months later it received a letter from its bank saying the transaction had been interrupted by the US treasury, which wanted more information on the transfer. The money eventually went through, but the incident raises important questions about the surveillance of financial transactions by the U.S. government. See Faisal al Yafai, "Palestinian Aid Groups' Accounts Closed", *The Guardian*, January 3, 2005. http://www.guardian.co.uk/print/0%2C3858%2C5094894-103690%2C00.html [March 5, 2005]; and Faisal al Yafai, "U-turn over Palestinian help group", *The Guardian*, January 10, 2005. http://www.guardian.co.uk/print/0%2C3858%2C5099255-103690%2C00.html [March 5, 2005].

[114] *Smart Border Action Plan, supra* note 61. See also, *Securing an Open Society: Canada's National Security Policy*, April 2004.

[115] Paul Weinberg, "Global agreements threaten media, privacy", *Rabble*, October 19, 2004. http://www.rabble.ca/news_full_story.shtml?x=34664 [November 24, 2004]. See also John Lettice, "Servers Seized By FBI Returned – but who wanted what?", *The Register*, October 14, 2004. http://www.theregister.co.uk/2004/10/14/indymedia_servers_back/ [March 5, 2005]. See also, John Lettice, "Home Office in frame over FBI's London server seizures", *The Register*, October 11, 2004. http://www.theregister.co.uk/2004/10/14/indymedia_servers_back/ [February 27, 2005].

[116] George Orwell, *Nineteen Eighty-Four*, 1949 (London, Penguin Classics: 2000), p. 5.

[117] Reg Whitaker, *supra* note 1, p. 25. Quotes are given in reverse order.

[118] *Ibid.,* p. 26, citing Owen Lattimore, *Ordeal by Slander* (Boston: Little, Brown, 1950).

[119] *Ibid*., p. 26.

[120] Michael Sniffen, "Controversial Terror Research Lives On", *Washington Post*, February 23, 2004. http://www.washingtonpost.com/wp-dyn/articles/A63582-2004Feb23.html [November 26, 2004]. [*Michael Sniffen*]

[121] *Ibid.*

[122] *Ibid*.

[123] *Ibid*.

[124] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 24. See also Shannon R. Anderson, "Total Information Awareness and Beyond: The Dangers of Using Data Mining Technology to Prevent Terrorism", Bill of Rights Defense Committee, July 2004. http://www.bordc.org/ [November 26, 2004]; and Associated Press, "Congress hides parts of U.S. spying project in other government agencies", *The Daily News* (Kamloops), September 26, 2003.

[125] Michael Sniffen, *supra* note 115.

[126] United States General Accounting Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548, May 2004. http://www.gao.gov/new.items/d04548.pdf. Cited in ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 24. The CIA and NSA did not participate in the GOA survey.

[127] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 24.

[128] Electronic Privacy Information Center, "Passenger Profiling: Overview", 2004. http://www.epic.org/privacy/airtravel/profiling.html [March 5, 2005].

[129] Sara Kehaulani Goo, "U.S. to Push Airlines for Passenger Records", *The Washington Post*, January 12, 2004, p. A01.

[130] Tim Harper, *supra* note 79.

[131] United States General Accounting Office, *Computer Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, February 2004. http://www.gao.gov/cgi-bin/getrpt?GAO-04-385 [November 26, 2004].

[132] Mimi Hall and Barbara DeLollis, "Plan to collect flier data canceled", *USA TODAY*, July 14, 2004.

[133] Sara Kehaulani Goo and Robert O'Harrow Jr., "New Airline Screening System Postponed; Controversy Over Privacy Leads to CAPPS II Paring, Delay Until After the Election", *The Washington Post,* July 16, 2004, p. A02. http://www.washingtonpost.com/wp-dyn/articles/A53320-2004Jul15.html [December 24, 2004]. [*Goo and O'Harrow*]

[134] Tim Harper, *supra* note 79.

[135] See Matthew L. Wald, "U. S. Wants Air Traveler Files for Security Test", *The New York Times*, September 22, 2004; and U.S. Department of Homeland Security, Transportation Security Administration, "TSA To Test New Passenger Pre-Screening System", Press Release, August 26, 2004. http://www.tsa.gov/public/display?theme=44&content=09000519800c6c77 [December 9, 2004].

[136] Ryan Singel, "Secure Flight gets wary welcome". Wired News, August 27, 2004. http://www.wired.com/news/privacy/0,1848,64748,00.html [March 6, 2005].

[137] Tonda MacCharles, "Air travellers face screening: Canadian program aims at terrorist 'risk scoring' system", *supra* note 54. Under the *Passenger Information (Customs) Regulations* [SOR/2003-219] of the *Customs Act*, Canada is collecting passenger information for incoming flights, and storing this information for analysis for six years. *The Public Safety Act, 2002* [2004, c. 15], allows the collection of passenger information for outgoing and domestic flights, as well as for incoming flights. The Canadian Risk Assessment Centre has access to the former and the latter. Beth Gorman, "Domestic passengers to be screened: Ottawa looking at kinds of information that can be collected", *Vancouver Sun*, January 31, 2004.

[138] Tonda MacCharles, *supra* note 58.

[139] Statewatch, "GERMANY: Police "trawling" for suspect foreigners", *Statewatch Bulletin*, vol. 12, no. 1 (Jan-Feb 2002), p 6.

[140] Goo and O'Harrow, *supra* note 133.

[141] Letter from Joseph Lieberman and Susan Collins of the U.S. Senate to The Honorable Asa Hutchinson, Under Secretary for Border and Transportation Security, U.S. Department of Homeland Security, dated April 14, 2004. The text of this letter is included in a press release of the Senate Committee on Governmental Affairs. http://govtaff.senate.gov/index.cfm?FuseAction=PressReleases.Detail&Affiliation=C& PressRelease_id=709&Month=4&Year=2004 [November 26, 2004].

[142] In 2002 the E.U. drew-up recommendations to the Council on the use of "terrorist profiling"… "putting together a set of physical, psychological or behavioural variables, which have been identified as typical of persons involved in terrorist activities and which may have some predictive value in that respect". See E.U. Council doc.: 11858/3/02 REV 3, 18.12.02. http://register.consilium.eu.int/pdf/en/02/st11/11858-r3en2.pdf. The UK and Germany are among a number of countries participating in an expert group on "terrorist profiling" with Europol . See E.U. Council doc.: 7846/04, 30.3.04. http://register.consilium.eu.int/pdf/en/04/st07/st07846.en04.pdf [February, 2005]. The E.U. is also apparently running a secret programme on "radicalism and recruitment", targeting Muslim communities' places of education and worship. The E.U. Network of Independent Experts in Fundamental Rights has serious concerns about the development of terrorist profiles. It argued that profiling by police or immigration authorities of potential terrorists on the basis of characteristics such as psycho-sociological features, nationality or birthplace "presents a

major risk of discrimination". It further argued that in order for profiling to be acceptable, a statistical link would have to be proven between the defined characteristics and the risk of terrorism, a link which at present has yet to be demonstrated. See E.U. Network of Independent Experts in Fundamental Rights thematic report 2003. http://www.statewatch.org/news/2003/apr/CFR-CDF.ThemComment1.pdf [December 2004].

[143] For Arar's story see Canadian Broadcasting Corporation, "Maher Arar: Statement", *CBC News Online*, November 4, 2003. http://www.cbc.ca/news/background/arar/arar_statement.html [March 5, 2005]. See also, pleadings in *Arar v. Ashcroft et al*. .http://64.233.167.104/search?q=cache:Kf5nduLfN4sJ:www.ccr-ny.org/v2/legal/september_11th/docs/ArarComplaint.pdf+Center+for+constitutional+rights+arar&hl=en [March 5, 2005].

[144] Solidarity Network, ATT0013.

[145] It was the same incident. See Testimony before the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Public Hearing, July 5, 2004. http://www.ararcommission.ca/eng/11e.htm [March 5, 2005]. Kate Jaimet, "Ottawa man left in legal limbo in Syria", *Ottawa Citizen*, July 10, 2004; Kate Jaimet, "The two worlds of Abdullah Almalki", *Ottawa Citizen*, July 10, 2004.

[146] Audrey Gillan, "Keep detainee in jail, appeal told", *The Guardian*, March 18, 2004. http://www.guardian.co.uk/terrorism/story/0,12780,1171876,00.html [December 9, 2004].

[147] *Smart Border Declaration, supra* note 61.

[148] *Smart Border Action Plan, supra* note 61, art. 25.

[149] Testimony of Garry James Loeppky before the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Public Hearing, June 30, 2004, pp. 807, 851, 885, 896-7. http://www.ararcommission.ca/eng/11e.htm [November 30, 2004].

[150] Testimony of Ward Elcock before the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Public Hearing, June 21, 2004, pp. 161, 251. http://www.ararcommission.ca/eng/11e.htm [November 30, 2004].

[151] CTV.ca News Staff, "Maher Arar suspects he's still being spied on", *CTV.ca*, September 9, 2004. http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1094738251010_90147450?s_name=&no_ads= [December 14, 2004].

[152] CBC News Online staff, "Man interrogated by CSIS, RCMP suing to clear his name", *CBC News Online*, October 3, 2004. http://www.cbc.ca/story/canada/national/2004/09/20/mohamed040920.html [December 14, 2004].

[153] Stephen Grey, "America's Gulag", *New Statesman*, Vol. 17, Issue 807, May 17, 2004. [*Stephen Grey*]

[154] "United Kingdom: Highest court to rule on indefinite detention", Human Rights Watch Press Release, October 1, 2004. http://www.hrea.org/lists/hr-headlines/markup/maillist.php [October 2004].

[155] Erich Lichtblau, "U.S. Opens 2 Inquiries Into Arrest of Muslim Lawyer in Oregon", *Newsweek U.S. Edition,* June 7, 2004.

[156] Andre Murr, "The Wrong Man; Brandon Mayfield speaks out on a badly botched arrest", *New York Times*, June 4, 2004. [*Andre Murr*]

[157] Al Goodman, "Spain hunts 'detonator bag' man", *CNN.com*, May 28, 2004. http://edition.cnn.com/2004/WORLD/europe/05/28/spain.warrant/ [December 14, 2004].

[158] Andre Murr, *supra* note 156.

[159] *Ibid.*

[160] *International Covenant on Civil and Political Rights*, 999 U.N.T.S. 171, art. 4. The ICCPR entered into force in the U.S. on September 8, 1992.

[161] 8 CFR 287, INS No. 2171-01, September 20, 2001.

[162] U.S. CONST., Amends. V and XIV. See also, ICCPR, art. 9.

[163] *County of Riverside v. McLaughlin*, 500 U.S. 44 (1991).

[164] Human Rights Watch Report, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees*, August 2002. http://www.hrw.org/reports/2002/us911/USA0802-05.htm [December 2004]. [*HRW, Presumption of Guilt*]

[165] David Cole, "Enemy Aliens and American Freedoms", *The Nation*, September 23, 2002. http://www.thenation.com/doc.mhtml?i=20020923&s=cole [December 30, 2004]. [David Cole].

[166] Cam Simpson, "U.S. Attorney General Won't Apologize for Treatment of Detained Foreigners", *Knight-Ridder Tribune*, June 6, 2003.

[167] *Ibid.*

[168] David Cole, *supra* note 165.

[169] Office of the Inspector General Report on Detainees, *supra* note 7. See also, *HRW, Presumption of Guilt, supra* note 158.

[170] *Center for National Security Studies v. U.S. Department of Justice*, 2002 U.S. District Court, Lexis 14168 (D.D.C., August 2, 2002), p. 28.

[171] *Hamdi v. Rumsfeld*, U.S. S. Ct. 03-6696, in which the court held the Executive has authority to detain Hamdi pursuant to a Congressional resolution authorizing the President to "use all

necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" or "harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons." Authorization for Use of Military Force ("the AUMF"), 115 Stat. 224.

[172] Mark Sherman, "U.S. told to charge or free suspect: Bush-appointed judge says government can't keep holding terror suspect after 2 ? years", *Associated Press*, March 1, 2005.

[173] Human Rights Watch, "UK: Freedom in the Balance – Britain's Highest Court to Rule on Indefinite Detention", Press Release, London, October 1, 2004. http://hrw.org/english/docs/2004/10/01/uk9421.htm [November 30, 2004].

[174] CBC News Online staff, "Security certificates constitutional: court", *CBC.ca News,* December 10, 2004. http://www.cbc.ca/story/canada/national/2004/12/10/security-certificate-041210.html [December 18, 2004].

[175] *Anti-Terrorism Act*, 2001, c.41, s. 83.3(4).

[176] Jake Rupert, "Government pays off victim of smear", *Ottawa Citizen*, October 2, 2003.

[177] *Ibid*.

[178] *Ibid*.

[179] See Statewatch, "No charges against Swedish Young Left donation to PLFP", Statewatch News Online, October, 2004. http://www.statewatch.org/news/2002/oct/11sweden.html [March 5, 2005]. [*Swedish Young Left*]

[180] American Civil Liberties Union, *Freedom Under Fire: Dissent in Post-9/11 America* (New York: ACLU, May 2003). http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12581&c=206 [December 18, 2004]. [*ACLU, Freedom Under Fire*].

[181] Randolph Bourne, "War is the Health of the State", from the first draft of an essay, "The State", which was unfinished at the time of Bourne's death in 1918. http://www.bigeye.com/warstate.htm [December 18, 2004].

[182] Frans Shor ,"The Crisis of Public Dissent", *Counterpunch Online,* September 9, 2004. http://www.counterpunch.org/shor09092004.html [December 18, 2004].

[183] Ian Hoffman, Sean Holstege and Josh Richman, "State monitored war protestors", *Oakland Tribune*, June 1, 2003. http://www.oaklandtribune.com/Stories/0,1413,82~1865~1400012,00.html [December 18, 2004].

[184] Ryan J. Foley, "Feds win Rights to War Protesters' Records", Associated Press, February 8, 2004.

[185] ACLU, *Freedom Under Fire*, *supra* note 180, p. 2.

[186] ACLU, *Freedom Under Fire, supra* note 180, pp. 5-6.

[187] Jeanne Meserve and Phil Hirschkom, "ACLU sues U.S. over 'no fly' list", *CNN.com*, April 6, 2004. http://www.cnn.com/2004/LAW/04/06/no.fly.lawsuit/ [December 14, 2004].

[188] Michelle Shephard, "How did this man land on a 'no-fly' list?; Air Canada 'flags' Toronto-born cartoonist; Airline has yet to address why it wouldn't sell ticket", *The Toronto Star*, June 15, 2004.

[189] CBS/AP, "Ted Kennedy's Airport Adventure", *CBSNEWS.com*, August 19, 2004. http://www.cbsnews.com/stories/2004/04/06/terror/main610466.shtml [December 14, 2004].

[190] Araminta Wordsworth, "If you're a David Nelson, you're a terrorism suspect", *The National Post*, June 23, 2003.

[191] Alexander Panetta and Jim Bronskill, "Legal concerns delay Canadian version of U.S.-style terror list for air passengers", *The Canadian Press*, distributed Oct. 31, 2004. http://www.cp.org/english/online/full/elxn_en/041031/p103104A.html [December 3, 2004].

[192] Ignacio Ramonet, "Terror Tactics", *Le Monde Diplomatique*, March 2004, referring to a report by PEN International, *Antiterrorism, writers and freedom of expression, London*, November 2003.

[193] Mark Bixler, "Carter Chides U.S. on Rights", *The Atlanta Journal-Constitution*, November 12, 2003.

[194] Amnesty International, "Colombia", *Amnesty Magazine*. http://www.amnestyusa.org/magazine/war_terrorism.html [March 6, 2005].

[195] Reid Morden, "Spies, not Soothsayers: Canadian Intelligence after 9/11", *CSIS Commentary*, No. 85, November 26, 2003. http://www.csis-scrs.gc.ca/eng/comment/com85_e.html [December 18, 2004].

[196] Available on the U.S. Department of Defense website, at http://www.defenselink.mil/news/Aug2004/commissions_instructions.html [March 6, 2005].

[197] Associated Press, "Anti-terror 'watchlists' merge to speed up access", *The Toronto Star*, September 17, 2004. See also documents obtained by the Electronic Privacy Information Center through a *Freedom of Information Act* request: http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html [December 18, 2004]. See also the testimony of FBI official Steve McCraw in "Can the Use of Factual Data Analysis Strengthen National Security? Part One", Hearing before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the House Committee on Government Reform, 108th Cong., May 6, 2003, Serial No. 108-72, p. 30. http://www.gpoaccess.gov/chearings/108hcat2.html [December 18, 2004].

[198] BBC News, "France 'confirms' fighter escorts", January 2, 2004. http://news.bbc.co.uk/1/hi/world/europe/3363291.stm [December 23, 2004].)

[199] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 19.

[200] James Gordon Meek, "13 Million on Terror Watch List", *New York Daily News,* April 8, 2003; Tom Godfrey, "5 million on [U.S.] terrorism list", *Toronto Sun,* January 20, 2004.

[201] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 20-21.

[202] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 19.

[203] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 19.

[204] See Brian Braiker, "The 'Patriot' Search*", Newsweek Online*, June 3, 2004, and correction. http://msnbc.msn.com/id/5131685/site/newsweek [December 18, 2004].

[205] The works of Czech writer Franz Kafka, published after his death in 1924, are notable for the recurrence of paradoxes or encounters with absurdity, and nightmarish predicaments. In *The Trial,* a man awakens one morning and, for reasons that are never clear, is arrested and subjected to the rigours of a mystifying judicial system for an unspecified crime. In *The Castle*, a land surveyor tries vainly to gain recognition from officials at a castle that dominates the life of a village. The word "Kafkaesque" has come to be used to describe situations characterized by surreal distortion, senselessness and often menacing complexity.

[206] Thomas Mathiesen, *On Globalistion of Control: Towards an Integrated Surveillance System in Europe*, *supra* note 5*,* p. 29.

[207] Canadian Foreign Affairs Minister Bill Graham met with U.S. ambassador Paul Celluci on October 15, 2002. Canadian Press, "Graham protests U.S. deportation of Canadian", October 17, 2002. http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1034846322080_44?s_name=&no_ads= [December 18, 2004]. Graham also raised Arar's case with U.S. Secretary of State Colin Powell in a meeting on November 14, 2002. Jeff Sallot, "PM trying to repatriate alleged al-Qaeda terrorist", *The Globe & Mail*, June 26, 2003. Prime Minister Jean Chrétien wrote to Syrian President Bashar Assad in July 2003 requesting Arar's release; the letter was hand-delivered to President Assad by Senator Pierre de Bané. Colin Freeze, "Arar freed after appeal from Chrétien: Former PM wrote letter to Syrian leader", *The Globe & Mail*, November 10, 2004. http://www.theglobeandmail.com/servlet/story/RTGAM.20041110.ARAR10_COPY/BNStory [December 19, 2004].

[208] See Swedish Young Left, *supra* note 179.

[209] When the European Commission finalized the deal amidst controversy, it "…argued that the alternative would have been chaos, with airlines facing fines and the loss of landing rights in the U.S., as well as trouble from E.U. data protection authorities." Ian Black, "E.U. hands over data on air travelers", *The Guardian*, May 18, 2004.

[210] Canada Department of Foreign Affairs and International Trade, *Fifth Annual Report on Canada's State of Trade, Trade Update: March 2004* (Minister of Public Works and Government Services Canada, 2004), pp. 3-4. http://www.dfait-maeci.gc.ca/eet/trade/state-of-trade-en.asp [December 19, 2004].

[211] Maude Barlow, *The Canada We Want – A Citizens' Alternative to Deep Integration* (Ottawa: Council of Canadians, n.d.). http://www.canadians.org/documents/TCWW_eng.pdf [December 19, 2004].

[212] Yap Swee Seng, SUARAM and the Asian People's Security Network, "Impacts on the South: The Case of Malaysia", *Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms and Democracy*, Report and Recommendations for Policy Direction of a Public Forum organized by the International Civil Liberties Monitoring Group (Ottawa: February 17, 2004), pp. 59-60. http://www.statewatch.org/observatory2ab.htm (Analysis No. 26) [December 15, 2004].

[213] Walden Bello, International Civil Liberties Monitoring Group International Conference held in Ottawa, February 17, 2004. [*Walden Bello*].

[214] Get cites see roch's email in South file with hyper links

[215] Walden Bello, *supra* note 213.

[216] *Farewell Radio and Television Address to the American People by President Dwight D. Eisenhower*, January 17, 1961. Available online at the site of the Dwight D. Eisenhower Library and Museum, http://www.eisenhower.utexas.edu/farewell.htm [December 3, 2004]

[217] Bob Davis, "Massive Federal R&D Initiative To Fight Terror Is Under Way," *The Wall Street Journal*, November 25, 2002, cited in ACLU, *The Surveillance-Industrial Complex, supra* note 77, p. 119.

[218] Statewatch, "E.U.: Security research programme to look at creating 'smart' biometric documents which will 'locate, identify and follow the movement of persons' through "automatic chips with positioning", *Statewatch News online*, February 2004. http://www.statewatch.org/news/2004/feb/23Aeu-plan-security.htm [December 23, 2004].

[219] For the full list of companies in the Group of Personalities, see "The Experts Looking Out for Europe's Security", *Intelligence Online*, No. 468. http://www.intelligence online.com/NETWORKS/FILES/468/468.asp?rub=networks [December 23, 2004].

[220] Commission of the European Communities, *Security Research: The Next Steps*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM (2004) 590 (Brussels: COEC, September 7, 2004), p. 10. http://europa.eu.int/eur-lex/en/com/cnc/2004/com2004_0590en01.pdf [December 23, 2004].

[221] Department of Finance Canada, *Enhancing Security for Canadians: Budget 2001,* http://www.fin.gc.ca/budget01/booklets/bksece.htm [December 23, 2004].

[222] ACLU, *The Surveillance-Industrial Complex*, *supra* note 77, pp. 26-28.

[223] Adam Mayle and Alex Knott, *Outsourcing Big Brother: Office of Total Information Awareness Relies on Private Sector to Track Americans*, Special report of the Center for Public Integrity, December 17, 2002. http://www.public-i.org/dtaweb/report.asp?ReportID=484 [December 19, 2004].

[224] Associated Press, "States build terror database resembling controversial federal project", *SiliconValley.com*, Sept. 23, 2003. http://www.siliconvalley.com/mld/siliconvalley/news/editorial/6841676.htm [December 19, 2004].

[225] Brian Bergstein, "U.S. Database Contractor Gave Authorities Names of 120,000 'Likely Terrorists'", Associated Press, May 20, 2004. http://cnews.canoe.ca/CNEWS/World/WarOnTerrorism/2004/05/20/467061-ap.html [December 19, 2004]. Public relations for Seisint have been handled by Qorvis Communications, which has received frequent media attention for representing Saudi Arabia. See Center for Media and Democracy, quoting "What Is the Matrix?", *O'Dwyer's PR Daily*, September 29, 2003. http://www.prwatch.org/node/2204 [December 19, 2004].

[226] CBS/AP, "U.S. Begins Tracking Foreigners", *CBS News*, January 5, 2004. http://www.cbsnews.com/stories/2004/01/05/terror/main591355.shtml [December 19, 2004].

[227] Lichtblau and Markoff, *supra* note 17.

[228] Greta Wodele, "Accenture Wins $10 Billion US VISIT Contract", *National Journal's Technology Daily*, June 1, 2004. http://www.govexec.com/dailyfed/0604/0604104tdpm1.htm [December 23, 2004].

[229] ACLU, *The Surveillance-Industrial Complex*, *supra* note 83, p. 28.

[230] Goo and O'Harrow , *supra* note 133.

[231] Richard Behar, "Never Heard of Acxiom? Chances Are It's Heard of You", *Fortune*, February 23, 2004. http://www.fortune.com/fortune/technology/articles/0,15114,588752,00.html [December 20, 2004].

[232] *Ibid.*

[233] European Commission, "Sweden to start issuing biometric passports and e-ID cards in 2005", *eGovernment News*, September 2, 2004. http://europa.eu.int/ida/en/document/3247/355 [December 24, 2004].

[234] European Commission, "Danish Government to start issuing biometric passports by the end of 2004", *eGovernment News*, February 18, 2004. http://europa.eu.int/ida/en/document/2164/333 [December 24, 2004].

[235] Canada News-Wire, *Canadian Air Transport Security Authority Pilot Project Includes Bioscrypt Technology,* February 23, 2004. http://www.newswire.ca/en/releases/archive/February2004/23/c2728.html [December 20, 2004].

[236] "Smart cards make inroads in Asia", *supra* note 38.

[237] Oki Electric Industry Co., Ltd., "Iris Recognition System is Selected for Border Control at Frankfurt/Main Airport by the German Federal Ministry of the Interior", Press Release, February 13, 2004. http://www.oki.com/en/press/2004/z03084e.html [December 24, 2004].

[238] BioDentity Systems Corporation website homepage, http://www.biodentity.com/ [December 24, 2004].

[239] Canada News-Wire, *Bahrain Enhances Border Security And Takes The Lead With E-Visas Using SITA Technology*, May 25, 2004. http://www.newswire.ca/en/releases/archive/May2004/25/c6965.html [December 20, 2004].

[240] Siemens Business Services, *Integrated ID Solutions*. http://www.siemens.nl/sbs/getfile.asp?id=97 [December 24, 2004].

[241] Thales Secure Operations, *People's Republic of China Uses Secure Identification Technology for Smart Card Based ID Card.* http://security.thalesgroup.com/case_study/case15.htm [December 24, 2004].

[242] Geoffrey York, "Rights Group Questions Trade Mission to China", *The Globe and Mail*, September 21, 2004.

[243] Barnaby J. Feder and Tom Zeller Jr., "Identity Badge Worn Under Skin Approved for Use in Health Care", *The New York Times*, October 14, 2004.

[244] Steven Lee Myers, "Opponents Call Putin's Overhaul Plan a Step Back", *The New York Times*, September 14, 2004.

[245] Jeremy Bentham, *The Panopticon Writings*, Miran Bozovic, ed.(London:Verso,1995) p. 29-95.

[246] Michel Foucault, *Discipline and Punishment: The Birth of the Prison*, Allan Sheridan, trans. (New York: Random House, 1995) at 261.

[247] Giorgio Agamben, Letter to the Editor [translation], *Le Monde*, January 11, 2004.

[248] Stephen Grey, *supra* note 153.

[249] See Anne Applebaum, *Gulag: A History* (New York: Anchor books, 2003).

[250] Stephen Grey, *supra* note 153; Estanislao Oziewicz, *supra* note 4. With respect to the CIA center in Jordan, see Associated Press, "Dozens of secret jails run by U.S., reprt says", *Toronto Star*, June 18, 2004. ["*Dozens of secret jails"*]. With respect to the CIA center in Qatar, see Jane Mayer, "Outsourcing Torture", *The New Yorker*, February 14, 2005. [*Outsourcing Torture*]

[251] Stephen Grey, *supra* note 153. See also U.S. State Department country reports.

[252] Stephen Grey, *supra* note 153.

[253] Stephen Grey, *supra* note 153.

[254] Estanislao Oziewicz, *supra* note 4. Another source put the number at 15,000 as of January 2004. Louise Christian, "Guantanamo: a global experiment in inhumanity", *The Guardian,* January 9, 2004. J. Cofer Black, former head of the CIA's Counterterrorist Center, testified in late 2002 that there were at least 3,000 terrorist prisoners being held worldwide. The Sudanese intelligence service alone claimed to have turned over more than 200 captives in the two years following September 11, 2001. Stephen Grey, *supra* note 153.

[255] Dana Priest, "Memo Okd Secret transfer of detaines: Experts say U.S. violated Geneva Conventions", *The Washington Post,* October 24, 2004.

[256] Association of the Bar of the City of New York and Center for Human Rights and Global Justice, *Torture by Proxy: International and Domestic Law Applicable to "Extraordinary Renditions"* (New York: ABCNY & NYU School of Law, 2004), p. 15. www.nyuhr.org/docs/TortureByProxy.pdf [December 20, 2004].

[257] Douglas Jehl, "Rule Change Lets C.I.A. Freely Send Suspects Abroad to Jails" New York Times, March 6, 2005. [*Jehl, "Rule Change*"] http://query.nytimes.com/search/query?ppds=bylL&v1=DOUGLAS [March 6, 2005]. The Directive is still classified.

[258] *Ibid.*

[259] Outsourcing Torture, *supra* note 250.

[260] According to officials, the CIA is authorized to do this under the new Directive. Jehl, "Rule Change", *supra* note 257.

[261] Kareem Fahim, "The Invisible Men", *The Village Voice,* March 30, 2004. http://www.villagevoice.com/issues/0413/fahim.php [December 20, 2004].

[262] Stephen Grey, *supra* note 153. See also, Christopher Bollyn, "The Pentagon's Ghost Planes and Enforced Disappearances", *American Free Press*, January 17, 2005. [*Christopher Bollyn*] referring to articles written in the *Sunday Times*, *Washington Post*, *Boston Globe* and *Chicago Tribune* trying to piece together facts about the fleet and its current operations.

[263] Stephen Grey, *supra* note 153.

[264] *Third Geneva Convention*, art. 122; *Fourth Geneva Convention*, art. 136.

[265] Art. 2(i).

[266] James Risen, David Johnston and Neil A. Lewis, "Harsh CIA Methods Cited in Top Qaeda Interrogaton", *The New York Times*, May 13, 2004.

[267] Outsourcing Torture, *supra* note 250.

[268] Human Rights Watch Briefing Paper, *The United States' "Disappeared": The CIA's Long-Term "Ghost Detainees",* October 2004, p. 8. [*Ghost Detainees*] "Army General Paul Kern told Congress that the C.I.A. may have hidden up to a hundred detainees." Outsourcing Torture, supra note 250.

[269] *Ghost Detainees*, supra note 268.

[270] Jonathan Steele, "Bush is now thinking of building jails abroad to hold suspects for life: a global gulag to hide the world's secrets", *The Guardian*, January 14, 2005. [*Jonathan Steele*]

[271] *Rasul v. Bush* USSCt No. 03—334. Decided June 28, 2004

[272] See, for example, David Rose, "How I entered the hellish world of Guantanamo Bay", *The Observer*, February 6, 2005. [*David Rose*]

[273] Testimony of Cofer Black, *Hearing Before the Joint Investigation of the House and Senate Intelligence Committees*, 107th Cong., Sept. 26, 2002. http://intelligence.senate.gov/0209hrg/020926/witness.htm [December 20, 2004].

[274] The U.S. has maintained that American constitutional guarantees for criminal process do not apply to the detainees there because they are aliens in foreign territory.

[275] The Bush Administration has alternately said that *Geneva Conventions* protections did not apply because the detainees were "unlawful combatants", that the *Geneva Conventions* did not apply to a war on terrorism, and that the *Geneva Conventions* did not apply because the Taliban was not the recognized government of Afghanistan and so not a party to the *Conventions*. See, Human Rights Watch, *Background Paper on Geneva Conventions and Persons Held by U.S. Forces, Human Rights Watch Press Backgrounder,* January 29, 2002. http://www.hrw.org/backgrounder/use/pow-bck.htm, referring to a statement made by Donald Rumsfeld on January 11, 2002. See also, Human Rights Watch, *Bush Errs in Geneva Convention Rules, Fails to Grant POW Status to Detainees,*

February 7, 2002. http://hrw.org/press/2002/02/geneva0207.htm; and Amnesty.International Report, *Human Dignity Denied:Torture and Accountability in the 'war on terror'*, October 27, 2004. http://web.amnesty.org/library/Index/ENGAMR511452004 [March 7, 2005]. [*Amnesty Human Dignity Denied*] [March 7, 2005]. Finally, see New York Times, "A Guide to the Memos on Torture", *The New York Times*. Http://www.nytimes.com/ref/international/24MEMO-GUIDE.html [March 7, 2005]. [*A Guide to the Memos on Torture*]. In particular, see descriptions of John C. Yoo's series of memorandums from January 2002 providing legal arguments to support the administration's assertions that the *Geneva Conventions* did not apply to detainees from the war in Afghanistan.

[276] A Guide to the Memos on Torture, *supra* note 275. In particular, see descriptions of a March 2003 memorandum declaring that President Bush was not bound by either international treaty prohibitions regarding the treatment of prisoners or by a federal anti torture law because he had authority as commander-in-chief to approve any technique to protect the nation's security; and letter to the ICRC from Brig. Gen. Janis, asserting that prisoners held as security risks could legally be treated differently from prisoners of war or ordinary criminals. Having taken prisoners to Guantanamo Bay from the theatre of war in Afghanistan and elsewhere, the U.S. has also maintained that, although it is a signatory to the *International Covenant on Civil and Political Rights*, the *Covenant* does not apply there because Guantanamo Bay is not U.S territory, but only leased by the U.S.

[277] Military Order of November 13, 2001, "Detention, Treatment and Trial of Certain Non-Citizens in the War against Terrorism" 66 F.R. 57833 (November 16, 2001); Department of Defense Military Commission Order No. 1, released March 21, 2002 and No. 2 released April 30, 2002; Department of Defense Military Instructions Nos. 1-8, released April 30, 2002.

[278] See *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

[279] In the 1949 *Geneva Conventions*, there are no categories other than civilians and combatants in the law. The *Third Geneva Convention* covers combatants in international hostilities and divides them into various subclasses.

[280] The Human Rights Committee has for some time held the view that a state bears obligations under the Covenant wherever it has jurisdiction, reading disjunctively the second "and" in Article 2 of the Covenant which provides, "Each State Party … undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant…".

[281] Art. 2.

[282] See in this regard Filartiga v. Pena-Irala, 630 F.2d 876 (2d Cir. 1980); Rodriguez Fernandez v. Wilkinson, 505 F. Supp. 787 (1980), aff'd on other grounds, 654 F. Supp. 1382 (10th Cir. 1981).

[283] John Barry, Michael Hirsh and Michael Isikoff, "The Roots of Torture", Newsweek, May 24, 2004. http://msnbc.msn.com/id/4989422/site/newsweek/ [December 20, 2004].

[284] Ibid.

[285] Outsourcing Torture, supra note 250.

[286] Ibid. See also, A Guide to the Torture Memos, supra note 275.

[287] Jonathan Steele, supra note 270.

[288] Human Rights Watch, Summary of Internatinal and U.S. Law Prohibiting Torutre and Other Ill-Treatement of Persons in Custody, May 24, 2004. http://hrw.org/english/docs/2004/05/24/usint8614_txt.htm [March 20, 2005]. See also, Amnesty, Human Dignity Denied, supra note ???

[289] David Johnston and Neil A. Lewis, "Bush's Counsel Sought Ruling About Torture", New York Times, January 5, 2005. [Johnston and Lewis]

[290] A Guide to the Memos on Torture, supra note 275.

[291] Ibid.

[292] Art. 2.

[293] Outsourcing Torture, supra note 250.

[294] A Guide to the Memos on Torture, supra note 275.

[295] Human Rights Watch, "U.S.: Did President Bush Order Torture?: White House Must Explain "Executive Order" Cited in FBI E-Mail", December 21, 2004. http://hrw.org/english/docs/2004/12/21/usint9925_txt.htm [December 2004]. [HRW, Did President Bush Order?]

[296] Johnston and Lewis, supra note 289.

[297] Outsourcing Torture, supra note 250.

[298] Art. 3.

[299] Dana Priest and Charles Babington, "Plan Would Let U.S. Deport Suspects to Nations That Might Torture Them", The Washington Post, September 30, 2004, p. A01.

[300] Estanislao Oziewicz, supra note 4.

[301] Estanislao Oziewicz, supra note 4. See also, Douglas Jehl, Steven Lee Meyers, and Eric Schmitt, "Abuse of Captives More Widespread, Says Army Survey", The New York Times, May 26, 2004, p. A1, citing American Army summary of deaths and mistreatment of prisoners in American custody in Iraq and Afghanistan; [Jehl, Meyers and Schmitt] Dana Priest and Barton Gellman, "U.S. Decries Abuse but Defends Interrogations", The Washington Post, December 26, 2002, p.

A01. [Priest and Gellman]. See also, Dozens of Secret Jails, supra note 250 which describes the case of a C.I.A. contractor who is accused of beating a detainee to death using his hands, feet and a flashlight.

[302] In December 2002, The Washington Post interviewed American national security officials who suggested that pain killers had been given selectively to Abu Zubaida, one of the top Al Qaeda leaders, who was shot in the groin during capture. See Priest and Gellman, supra note 301.

[303] Priest and Gellman, supra note 301. See also, Tim Golden and Eric Schmitt, General took Guantanamo rules to Iraq for Handling of Prisoners", The New York Times, May 13, 2004. [Golden and Schmitt]

[304] Priest and Gellman, supra note 301. See also, Golden and Schmitt, supra note 303.

[305] Priest and Gellman, supra note 301.

[306] Associated Press, "37 deaths of detainees in Iraq, Afghanistan probed", Sunday Observer Online, May 23, 2004.

[307] Dan Eggen and R. Jeffrey Smith, "F.B.I. agents allege abuse of detainees at Guantanomo Bay", The Washington Post, December 21, 2004.

[308] As of May, 2004, the Army had closed two homicide cases. One involved an Iraqi detainee who had been shot for throwing rocks at guards. Jehl, Meyers and Schmitt, supra note 301.

[309] Neil A. Lewis, "Broad Use of Harsh Tactics", The New York Times, October 17, 2004.

[310] Jehl, Meyers, and Schmitt, supra note 301.

[311] Associated Free Press, "C.I.A. renditions of suspects are 'out of control'", The Nation on web, 2004.

[312] David Rose, supra note 272.

[313] HRW, Did President Bush Order?, supra at note 295.

[314] Ibid. A Guide to the Memos on Torture, supra note 275.

[315] A Guide to the Memos on Torture, supra note 275.

[316] Scott Highman and Joe Stephens, "New Details on Scale of Iraq Prison Abuse", The Washington Post, May 21, 2004.

[317] Carl Huse and Sheryl Gay Stolberg, "Lawmakers View Images from Iraq" The New York Times, May 13, 2005.

[318] Ibid.

[319] Ibid.

[320] Eric Schmitt, "Rumsfeld and a General Clash on Abuse", The New York Times, May 12, 2004.

[321] Kate Zernike, "Accused Soldier Paints Scene of Eager Mayhem at Iraqui Prison", The New York Times, May 14, 2004.

[322] Jehl, Myers and Schmitt, supra note 301.

[323] Associated Press, "39 have died in U.S. hands: misconduct condoned, report says", The Toronto Star, July 23, 2004.

[324] Outsourcing Torture, supra note 250.

[325] Jonathan Steele, supra note 270.

[326] Ibid.

[327] Ibid.

[328] Ibid.

[329] Douglas Jehl, Pentagon Seeks to Transfer More Detainees from Base in Cuba, The New York Times, March 11, 2005. See also, Dawn, "Life Imprisonment without trial condemned", January 3, 2005. http://www.dawn.com/2005/01/03/int1.htm [March 20, 2005].

[330] Tony Johansson, "A Scandal in Sweden", Z-Net, May 25, 2004.

[331] Stephen Grey, "U.S. agents 'kidnapped militant' for torture in Egypt", Timesonline, February 6, 2005.

[332] James Meek, "They beat me from all sides", The Guardian, January 14, 2005. See also, James Gordon, "German's tale eerily similar to Arar's: Man said he was abducted, flown to Kabul where he claims U.S. officials tortured him.", Ottawa Citizen, January 12, 2005.

[333] Human Rights Watch, Empty Promises: Diplomatic Assurances No Safeguard against Torture, April 2004. http://hrw.org/reports/2004/un0404/ [March 31, 2005].

[334] Human Rights Watch Briefing Paper for the 59th Session of the United Nations Commission on Human Rights, In the Name of Counter-Terrorism: Human Rights Abuses Worldwide, March 25, 2003. http://hrw.org/un/chr59 [March 31, 2005]. [HRW, In the Name of Counter-Terrorism]

[335] Ibid.

[336] Ibid.

[337] Ibid.

[338] Ibid.

[339] Human Rights Watch, "Malaysia: Detainees Abused Under Security Law", Press Release, May 25, 2005.

[340] Human Rights Watch, In the Name of Security: Counter-terrorism and Human Rights Abuses Under Malaysia's Internal

Security Act, May 2004, Vol. 16, No. 7 (C), p. 44.

[341] Ibid., p. 43.

[342] Ibid., p. 45.

[343] Ibid., p. 44.

[344] Ibid.

[345] Ibid.

[346] Ibid., p. 43.

[347] Christopher Bollyn, supra note 262.

[348] Outsourcing Torture, supra note 250.

[349] Christopher Bollyn, supra note 262.

[350] Jim Lobe, "U.S. Militarizing Latin America", OneWorld.net, October 6, 2004.

[351] Jack Epstein, "General Seeks Boost for Latin American Armies", San Francisco Chronicle, April 30, 2004.

[352] HRW, In the Name of Counter-Terrorism, p. 12.

[353] David Corn, "The 9/11 Investigation", The Nation, August 4, 2003. http://www.thenation.com/doc.mhtml%3Fi=20030804&s=dcorn [December 21, 2004].

[354] Mark Trevelyan, "Head of Interpol highlights abuses in war on terror", Statewatch News online, October 2, 2003. http://www.statewatch.org/news/2003/oct/05interpol.htm [December 21, 2004].

[355] Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence Together With Additional Views, December 2002. http://www.gpoaccess.gov/serialset/creports/911.html [December 21, 2004]. [Joint Inquiry Report].The Joint Inquiry referred to a long list of intelligence findings, which indicated that Al Qaeda was eager to attack the United States and that terrorists were interested in using airplanes as weapons. These included an intelligence briefing, prepared in July 2001, that said that bin Laden was looking to pull off a "spectacular" attack against the United States designed to inflict "mass casualties" and that "[a]ttack preparations had been made". A summer 1998 intelligence report suggested bin Laden was planning attacks in New York and Washington, and in September 1998, the head of the C.I.A. briefed Congress and noted that the F.B.I. was following three or four bin Laden operatives in the U.S. In December 1998 an intelligence source reported that an Al Qaeda member was planning operations against U.S. targets: "Plans to hijack US aircraft proceeding well. Two individuals … had successfully evaded checkpoints in a dry run at a NY airport". In December 1999, the C.I.A.'s Counter-terrorism Center concluded that bin Laden wanted to inflict maximum casualties, cause massive panic and score a psychological victory. To do so, it said, he might attack between five and 15 targets on the Millennium, including several in the United States. In 2000, the C.I.A. had information that two of the 9/11 hijackers who had already been linked to terrorism were, or might be in the United States. In April 2001, an intelligence report said that Al Qaeda was in the throes of advanced preparation for a major attack, probably against an American or Israeli target. In August 2001, the F.B.I. began to try to locate the two hijackers mentioned above.

[356] Ibid., p. 7.

[357] Ibid., pp. 7, 33.

[358] Ibid. One intelligence source informed the Joint Inquiry that "a closely held intelligence report" for "senior government officials" in August 2001 stated that bin Laden was seeking to conduct attacks in the U.S., that Al Qaeda maintained a support structure there, and that information obtained in May 2001 indicated that a group of bin Laden supporters were planning attacks in the United States with explosives. (p. 9). The Joint Inquiry's report also notes that in May 2001, "the U.S. Government became aware that an individual in Saudi Arabia was in contact with a senior al-Qa'ida operative and was most likely aware of an upcoming al-Qa'ida operation." (p. 111)

[359] David Corn, supra note 353.

[360] Richard Ford, "Safeguards promised after Big Brother warning by watchdog", The Times, August 16, 20. http://www.timesonline.co.uk/article/0,,2-1219015,00.html

[361] See GILC website, http://www.gilc.org/index.html.

[362] See EDRi website, http://www.edri.org/.

[363] Privacy International, Invasive, Illusory, Illegal and Illegitimate: Privacy International and EDRi's Response to the Consultation on a Framework Decision on Data Retention, September 15, 2004. http://www.statewatch.org/news/2004/sep/data-retention.htm [March 5, 2005}.

[364] Ibid.

[365] Open Letter to ICAO, supra note 38; Transferring Privacy, supra note 55.

[366] See for example, U.K. No2Id Campaign, http://www.no2id.org/ [March 6, 2005].

[367] Joint Declaration on the Need for an International Mechanism to Monitor Human Rights and Counter-Terrorism, signed by the Coalition of International Non-Governmental Organizations against Torture. http://www.geneva.quno.info/pdf/CounterTerrorismDecl.pdf [March 1. 2005].

[368] See http://www.aclu.org/privacy.

[369] See http://www.aclu.org/Privacy/Privacy.cfm?ID=14729&c=130 [March 6, 2005].

[370] See http://www.aclu.org/matrix [March 6, 2005].

[371] See http://www.aclu.org/capps [March 6, 2005].

[372] See http://aclu.org/SafeandFree/SafeandFree.cfm?ID-15422&c=206 [August, 2004].

[373] See ACLU, Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society. http://aclu.org/monster [March 6, 2004]; Unpatriotic Acts:The FBI's Power to Rifle Through Your Records and Personal Belongings Without Tellling You http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13246&c=206 [August 2004].

[374] Statewatch, "International Conference of Data Protection and Privacy Commissioners adopt series of resolutions calling for global standards" Statewatch News Online, September 2003. http://www.statewatch.org/news/2003/sep/12audata.htm.

[375] Hana Stepankova, "Czech Office for Personal Data Protection, on handing over personal passenger data to the USA", Prague Post, November 12, 2003.

[376] See note 126 and 131.

[377] See note 7.

[378] Bill of Rights Defense Committee, "372 Civil Liberties Safe Zones!". http://www.bordc.org/ [March 6, 2005].

[379] Agence France-Presse, "L'Inde abrogera une loi anti terroriste", Le Monde, 27 mai 2004. http://www.cyberpresse.ca/monde/article/1,151,1063,052004,693484.shtml [March 6, 2005].

[380] A(FC) and others (FC) v. Secretary of State for the Home Department; X(FC)) and another (FC) v. Secretary of State for the Home Department, [2004] UKHL 56 (December 16, 2004

[381] Ibid., para. 74.

[382] Ibid., paras. 96 and 97.

[383] (03-334). "Since the Supreme Court ruling, the government has begun holding 'combatant status review tribunals'at Guantanamo Bay for each detainee to determine whether he should continue to be held. The detainees do not have legal representation at those hearings. So far, 317 hearings have been held and 131 cases have been adjudicated, all but one in favour of continued detention."

[384] See also, Neil A. Lewis, "Judge Says Terror Suspect Can't be held as an Enemy Combatant", New York Times, March 1, 2005.

[385] Carol D. Leonnig and John Mintz, "Judge Says Detainees' Trials are Unlawful", The Wahsington Post, November 9, 2004.

[386] Doe and ACLU v. Ashcroft et al., No. 04-CIV-2614 (District Court, 2d Cir.). See also, Dan Eggen, "Key part of PATRIOT ACT ruled unconstitutional", The Washington Post, September 29, 2004.

[387] For a list of these, see International Commission of Jurists, E-BULLETIN ON COUNTER-TERRORISM & HUMAN RIGHTS, No. 2, September 2004, p.2. http://www.icj.org/IMG/pdf/E-bulletinSept.pdf [March 5, 2005].

[388] Dan Eaton and Muklis Ali, "Indonesian anti terror law declared invalid, Reuters, July 23, 2004.

[389] Christian Schröder and Cédric Laurant, "Austrian Federal Constitutional Court, VfGH G37/02 ua, February 27, 2003 - Outline", Electronic Privacy Information Center. http://www.epic.org/privacy/intl/austrian_vfgh-022703.html [March 6, 2005].

[390] EDRi, "Change in Germany's position on data retention", October 6, 2004. http://www.edri.org/edrigram/number2.19/retention

International Campaign Against Mass Surveillance