
# International Campaign Against Mass Surveillance (ICAMS)

April 20, 2005

**International Campaign against Mass Surveillance**

The unprecedented assault on the rights to privacy, freedom of expression and freedom of movement requires an equally unprecedented response by civil society around the world.

The *International Civil Liberties Monitoring Group*, that represents some thirty civil society groups, joined other well-known human rights groups from around the world – the American Civil Liberties Union (US), Statewatch (G-B), and Focus on the Global South (Philippines) -- in launching an the ***International Campaign Against Mass Surveillance***, which calls on governments to put an end to massive surveillance and global registration of entire populations.

Patterned in some respects after the international campaign to ban landmines, the ***International Campaign Against Mass Surveillance*** is aimed at building a movement of resistance to these measures around the world by circulating a core document, this summary of the latter and a declaration for endorsement.

You can consult the documents, see the list of supporting groups and organizations to date and endorse the declaration on line on the campaign website. If you wish to endorse the campaign but do not have easy access to internet, please contact the *Ligue des droits et libertés* at 514-849-7717.

## Campaign Web site: www.i-cams.org

# THE EMERGENCE OF A GLOBAL INFRASTRUCTURE FOR MASS REGISTRATION AND SURVEILLANCE

## Executive Summary

Global security and the "war on terror" now dominate the global political agenda. Driven largely by the United States, a growing web of anti-terrorism and security measures are being adopted by nations around the world. This new "security" paradigm is being used to roll back freedom and increase police powers in order to exercise increasing control over individuals and populations.

Within this context, governments have begun to construct, through numerous initiatives, what amounts to a global registration and surveillance infrastructure. This infrastructure would ensure that populations around the world are registered, that travel is tracked globally, that electronic communications and transactions can be easily monitored, and that all the information that is collected in public and private databases about individuals is stored, linked, data-mined, and made available to state security agents.

The object of the infrastructure is not ordinary police work, but mass surveillance of entire populations. In its technological capacity and global reach, it is an unprecedented project of social control. Already, the United States and other countries are aggressively using information gathered and shared through this infrastructure to crack down on dissent, close borders to refugees and activists, and seize and detain people without reasonable grounds.

And, all of this is taking place at a time when the U.S. and its allies are maintaining a system of secret and extraterritorial prisons around the world, in which unknown numbers of prisoners are facing indefinite, arbitrary detention and torture.

It is time for the public to take stock of the road that governments are leading us down with these new registration and surveillance initiatives. The ten "signposts" described below show just how far down the road we have already traveled, and the dangers that lie ahead for all of us if we fail to make governments turn back.

### 1st Signpost: The Registration of Populations

The *first signpost* on the road governments are leading us down was the effort by the United States after September 2001 to register male non-citizens from designated countries, and then all foreigners traveling to the U.S., and similar efforts by the European Union to register immigrants and travelers.

In the United States, this happened under two programs called NSEERS and US-VISIT.

- **NSEERS.** Under NSEERS (National Security Entry-Exit Registration System), male non-citizens over the age of 16 from designated (mostly Muslim) countries were required to register with the federal government. The more than 80,000 individuals who registered reported many stories of harassment, insult, and rough treatment. NSEERS resulted in more than 13,000 people being put into deportation hearings and thousands more fleeing the country in fear.
- **US-VISIT.** NSEERS was eventually phased out, but that has hardly resulted in an end to the registration of foreigners; it was replaced by another program called US-VISIT, under which *all* visitors (except some Mexicans and most Canadians) are to be digitally photographed and fingerprinted upon or prior to their entry into the United States. This data will not be used merely for authentication checks, but will be linked to over 20 U.S. federal government databases as well as to unknown other sources of information. Combined with that data, the US-VISIT biometric data will form the seed of a vast new system of dossiers on international travelers.

In Europe, similar registration and data linkage is occurring with the creation of the new EU Visa Information System (VIS) and an EU-wide foreigners' register:

- **EU-VIS.** Under the new EU VIS system, the information on every visa application to the 25 EU member states, including the photographs and fingerprints of individuals, will be recorded in a central database. These records will be accessible to law enforcement and security agencies across the EU.
- **"EU-wide foreigners' register".** Additionally, registers of all legally resident third-country nationals are being created through the "harmonization" of residence permits in the EU member states. This data will be stored in a central EU database. An automated procedure will link this database and the new EU VIS database to other EU databases.

## 2nd Signpost: The Creation of a Global Identification System

The *second signpost* is what amounts to the domestic counterpart of the registration of foreigners: the creation by governments of an international identity card system for *citizens*.

National ID cards – and more significantly, the databases that lie behind them – not only provide a means of registering domestic populations, but they also provide a centralized, standardized means for tracking people as they go about routine life activities. In many democracies, the idea of a national identity card has been anathema due to its strong association with police states. 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.

Since September 2001, many countries around the globe have started or intensified efforts to institute national ID databases; countries that already have national IDs are in many cases exploring ways of extending their capabilities and their use.

But overtaking this trend is the emergence of a new identity tool that is being implemented in all countries: the "globally interoperable biometric passport." Based on an international standard created at the urging of the United States, nations around the world are in various stages of adopting passports that contain biometrics such as digital photographs and fingerprints, as well as RFID chips capable of broadcasting that information to anyone with an reader. The United States has informed its allies that if they do not adopt these passports, their citizens will no longer be permitted to enter the U.S. without a visa.

The upshot is that individuals around the world are being issued computerized identity documents, and entered into identity databases in their own and other countries, setting the stage for the mass, routinized surveillance of individuals' movements.

## 3rd Signpost: The Creation of an Infrastructure for the Global Surveillance of Movement

The *third signpost* is the creation of a global infrastructure for the surveillance of movement. Not only are the authorities of many nations well on the way toward constructing checkpoints and databases to track individuals' movements using their national identity documents and/or biometric passports, they are also seeking direct access to airlines' passenger name records (PNR).

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

The United States government, in particular, has demanded access to this information, forcing airlines to turn it over even when it would violate the privacy laws that protect passengers in the European Union and other nations around the globe. After extended negotiations, the U.S. succeeded in pressuring EU officials to betray their own privacy principles and enter into a formal agreement with the U.S. giving it access to European PNR. The European Union, meanwhile, has decided to set-up its own PNR system to record the movement of everyone traveling in and out of the EU.

The International Civil Aviation Organization (ICAO), a UN body, is currently considering a harmonized data format for PNR, encouraging states around the world to establish their own PNR systems and to share data globally. Information about where individuals fly, and how often (together with very personal information such as ethnicity

and hotel sleeping arrangements), will be tracked, stored, and shared between countries, and used to regulate and control the movement of people across borders.

## 4th Signpost: The Creation of an Infrastructure for the Global Surveillance of Electronic Communications and Financial Transactions

The *fourth signpost* is the creation of an infrastructure for the global surveillance of electronic communications and financial transactions. That includes a number of developments, including:

- **Expanded legal authorities for eavesdropping.** Through measures such as the American "Patriot Act," the United States as well as other nations around the world have responded to the events of September 11 by expanding government powers to read e-mail and eavesdrop on conversations and other electronic communications, and by weakening judicial oversight over those powers.
- **Expanded private-sector requirements.** Governments are also imposing more requirements on companies and other private-sector entities to ensure that surveillance is technically possible and easy to do. Some governments are claiming they must introduce these requirements to comply with the Convention on Cybercrime – a treaty that has been pushed by the United States since 9/11 and would give the authorities broad new powers to investigate computer-related crime across national borders.
- **Mandatory "data retention":** Governments, particularly those in Europe, are also pushing for "mandatory data retention," under which all communications service providers will be required to save and store data on their consumers that they would otherwise erase in accordance with privacy laws. The EU is currently discussing binding legislation that will require the mandatory retention of all telephone, e-mail, fax and internet traffic data for up to three years.
- **The expansion of ECHELON.** A shadowy and little-understood international surveillance program codenamed Echelon soaks up much of the world's electronic communications. A partnership between the United States, the U.K., Canada, Australia, and New Zealand, Echelon allows each country to avoid domestic judicial oversight over surveillance by asking the others to spy on its citizens. With new requirements in many countries regarding the retention and collection of data, far more information will presumably be available to Echelon in the future.
- **Tracking and reporting of financial transactions.** New laws around the world enlist financial institutions and ordinary businesses into a financial-surveillance infrastructure under the justification of stopping money-laundering and the financing of terrorism. For example:
    - A post-9/11 U.N. Security Council resolution requires all states to prohibit their citizens from making funds or services available to terrorists – a mandate that all but requires mass surveillance of economic activity.

- In the United States, the "Patriot Act" has built up a vast legal-bureaucratic machinery for the systematic gathering and analysis of financial transactions.
- The FATF (Financial Action Task Force), a multilateral policy-making body with 31 member countries, has extended its mandate from money-laundering to terrorist financing, and the Organization for Economic Cooperation and Development (OECD) has followed suit.

Through these initiatives, state agents from around the world are rapidly gaining direct, cost-free access to every e-mail and phone call made, every website visited, and every financial transaction conducted. Charities and NGOs working in conflict zones, or with links to Arab and Muslim communities, are already experiencing the chill of this new infrastructure.

## 5th Signpost: The Convergence of National and International Databases

The *fifth signpost* is a development that feeds into all of the others: the convergence of diverse databases –government and private-sector, nationally and internationally. This trend is happening on many different levels. Examples include:

- The U.S. effort to tie over 20 different government databases into the US-VISIT system
- The collection and conglomeration of personal information about U.S. citizens and the citizens of other countries by giant corporate data brokers in the U.S. and the purchase of this data by dozens of U.S. government agencies
- The tying together of numerous government and private-sector data sources into a single comprehensive view by programs like the one called "the MATRIX" in the U.S., which is then made available to police across the country

The convergence of data from different sources into single centralized (or distributed but centrally accessible) databases turns data collection into full-fledged surveillance by providing ever-more-comprehensive records of individuals' activities across time. The result is 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 dossiers on everyone.

## 6th Signpost: The Spread of the "Risk Assessment" Model

The *sixth signpost* is the spread of a "risk assessment" paradigm that is driving the collection, storage and linkage of so much information. Under this approach to security, personal information is collected *en masse* about individuals so that a judgment can be made about their "trustworthiness" or risk to security. Instead of focusing on time-honored techniques of working outward from known facts and suspected wrongdoers, the

risk assessment approach seeks to subject *everyone* to scrutiny, in the hopes of combing wrongdoers out of the crowd.

The *high tech* approach to sorting for "risk" through the ocean of information that is being collected by mass surveillance, is to use computer "data mining" programs that search for suspicious patterns of activity. This is like looking for a needle in an ocean of needle haystacks. Not surprisingly, these programs yield alarmingly high error rates – not only in the innocent people they flag as "dangerous", but in the dangerous people they fail to flag. The *low tech* approach to risk assessment is to have human beings making on the spot judgments about who they think presents a "risk" to society. But since human beings are encouraged to err on the side of caution and disregard the welfare of the individuals involved, the stories of innocent people being wrongly assessed in this way are mounting.

Risk assessment has truly Kalfkaesque implications because the criteria used for making judgments are vague or undisclosed and the information used is often inaccurate or incomplete. Innocent individuals who are labeled security risks under the risk assessment model are usually given no indication of why that label was applied and how they can remove it.

## 7th Signpost: Security-Force Integration and the Loss of Sovereign Checks and Balances

The *seventh signpost* is the deep integration of countries' police, security, intelligence, and military establishments, and the concomitant abandonment of national sovereignty and control. Examples of this trend include:

- The growing number of "mutual assistance agreements" pledging cooperation between law enforcement and security agencies from different countries. Recently such an agreement was cited by U.S. officials who seized computer servers in London hosting the websites of *Indymedia* (the Independent Media Centre) in twenty countries, purportedly at the request of the Swiss and Italian police.
- The joint investigation teams being set up between the U.S. and Canada, and the U.S. and the 25 member states of the EU. These teams share information without formal state-to-state requests under mutual assistance agreements, and may be legally unaccountable for their actions on foreign soil. Such teams can include customs, police and immigration agents, as well as agents from security and intelligence organizations.
- The agreement between Europol and the United States, concluded without democratic oversight, which 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 life of individuals. The agreement was signed despite its violating the *Europol Convention* and the EU *Data Protection Directive*.

- Mounting stories showing the inability of governments to protect their own citizens when they are wrongly caught up in the global security net, as in the case where the Canadian government tried to obtain the release of a Canadian citizen whom the U.S. had rendered to Syria, or the case where the Swedes tried to have some of their citizens' names removed from U.N. terrorist list and had to negotiate with the U.S.

## 8th Signpost: The Corporate Security Complex

The *eighth signpost* is the creation of a new "corporate security complex." In the computer age, an ever-larger proportion of our activities are being tracked and recorded by private companies, and that information is increasingly available to governments. Government powers to demand access to such data are being expanded, but many businesses are also voluntarily selling databases and other services to government agencies.

For technology and data companies, the "war on terror" has opened up a new government customer base. For government security and intelligence agencies, left searching for a *raison d'être* after the end of the Cold War, the "war on terror" has offered an unprecedented opportunity to increase its investigative and surveillance powers. This new corporate security complex has become an aggressive driver of the global surveillance project.

Multinational corporations based in the U.S, Western Europe and Asia are poised to make huge profits from the global market for databases, biometric readers, data mining programs and other new technologies of control.

The EU has established a new "security research agenda", intended to make the EU the rival of the U.S. in security technology. One of its objectives is to break down the barrier between civil and military research so that both can serve military, economic and foreign policy ends. Canada, too, has channeled billions into surveillance and security technology. The major surveillance projects undertaken by the United States such as the U.S. VISIT, MATRIX, CAPPS II and Terrorism Information Awareness programs, have offered a veritable goldmine of business opportunities to technology companies. Corporations have been quick to seek relationships with security apparatuses in these countries and elsewhere and to peddle more and more intrusive technologies of control.

## 9th Signpost: The Erosion of Democratic Values

The *ninth signpost* is the dismaying betrayal of democratic values by the government of the United States and other democracies as they move to implement the global surveillance project. In order to achieve their ends, governments have:

- suspended judicial oversight over law enforcement agents and public officials
- concentrated unprecedented power in the hands of the executive arm of government
- circumvented the democratic oversight and debate normally provided by the legislative arm of government by imposing policy through unelected, unaccountable transnational bodies
- steamrolled over well-established privacy protections for citizens
- ignored constitutional guarantees and rolled back criminal law and due process protections that balance the rights of individuals against the power of the state (such as the presumption of innocence, *habeas corpus*, attorney-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)
- undermined freedom of expression and association

Where mass registration and surveillance measures have been adopted by repressive regimes, they have bolstered or worsened the status quo. The example set by Western nations allows governments in less democratic countries to consolidate their grip on power and gives them a green light to commit human rights and other abuses.

## 10th Signpost: Rendition, Torture, Death

The *tenth signpost* is the loss of moral compass on the part of the United States and other countries that hold themselves out as defenders of human rights as they have begun to embrace inhumane and exceptional practices of social control. It is now clear that the U.S. and other countries are engaging in torture, inhumane treatment and indefinite detention of detainees in the "war on terror" in their own facilities, as well as sending suspects to third countries where they face similar or worse abuses. The worst that individuals have to fear from the global surveillance system is something far darker than mere loss of privacy, civil liberties, or freedom of movement.

The United States is operating a system of prison camps and detention centers around the world that remains largely unseen by the world. Some of these are being run directly by the U.S. – including Guantanamo Bay in Cuba and other detention centers in Afghanistan, Iraq, Qatar, Pakistan, Thailand and elsewhere. Other prisons are run by cooperating agencies in Jordan, Morocco, Saudi Arabia, and Pakistan – countries with documented records of using torture in interrogation. Among the worst are facilities in Damascus, Syria, where Canadian Maher Arar was held, and in Cairo.

The Bush Administration has asserted that neither American criminal law, nor the Geneva Conventions, nor other international laws apply to the people swept up into this system of camps. In other words, according to the United States, these detainees exist in a legal "black hole": 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. While international law and the laws of most nations (including the United States) clearly bar the use of torture on *anyone*, this development is doubly chilling given the fact

that many victims are proving to be innocent of ties to terrorism. The sordid record of torture, extra-legal renditions, and even extra-judicial killing amount to betrayal of democratic values and of civilization itself.

## Conclusion

When one examines all of the developments described above, it becomes apparent that the road toward a global infrastructure for mass registration and surveillance is a dangerous one, both for our personal and our collective security.

The initiatives described in this report are not effective in flagging terrorists or stopping their determined plans. They divert crucial resources away from the kind of investments in human intelligence we need to give us good intelligence about specific threats, rather than useless information on the nearly 100 percent of the population that poses no threat whatsoever. They alienate the very communities from whom intelligence agencies need assistance in order to obtain good intelligence. They do nothing to address the root causes of terrorism. Far from making us personally safer, they weaken the democratic institutions and individual protections upon which citizens' security depend. Far from making the world a safer place to live in, they exacerbate global insecurity. Their unjust targeting of Muslims and the brutal, lawless treatment meted out in the global network of detention camps described above engender hatred against Western countries and their partners, fomenting only more fanatical oppositions and terrorism.

We are less safe with mass registration and surveillance, not more.

It is time for the public to take action! People around the world must tell our governments that they are on the wrong track. Add your voice to the **International Campaign Against Mass Surveillance** by signing the **Declaration**.