

International Campaign Against Mass Surveillance

**THE EMERGENCE OF A
GLOBAL INFRASTRUCTURE**

10th ICJNGPOT: A LOOK OF MORAL COMPASSION – ENDEAVOUR, TORTURE, DEATH	39
1. The Global Gulag	39
a) Detention Centres Used by The ICJ	39
b) The Practice of Torture	40

THE ROAD WE ARE HEADI G D W

O

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

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*

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 SIG ST: THE REGISTRATI
F ULATI S**

In 1930s Germany, the Holocaust began with the

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 follow-

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,

were then given to the Pentagon and com-

information other than biometrics on chips, to

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

f) Expansion to other Transportation

- retention of data only as strictly required for a declared use

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,

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” Surveillance⁸³ 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

them to preserve information in their systems) are another.⁹⁰ Alarminglly, another aspect of the *Convention* is the requirement, in some circumstances, to provide mutual assistance to co-signatories even where the activity to be inves-

In 1948, the U.S., the U.K., Canada, Australia and New Zealand created a program under which they trawled the world's telephone commu-

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, whenever 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

eIOT(r[(D)strationten) Tj0 -1.31.2 TD02.01 Tc00.03 TwConv[(D)o tel(, ac(of)e Siac(of)e 9/11Act) TJETB

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 infor-

overseas or against non-Americans within the U.S. But there is nothing to stop the government from expanding this program to American citizens

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

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 untrue¹⁴¹ 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

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 trans-

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 o5t1cf in the first place”.¹⁵³

The English Courtt1c Appeal ruled in August 2004 that the uset1c evidencet1btained onder torture was legal in the U.K., as long as the U.K. neither “procured nor connived at” torture.¹⁵⁴

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

e) Broad Strokes: The U. . 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

documented numerous instances in which U.S. authorities have made extremely questionable risk assessments, targeting citizens who have

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 coordinator¹⁸⁷ have also been among the many passengers pulled aside under the U.S. “i5scly” 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 Tm0.123 Tw[(The “i5scly” list is run by the)19(T)36(ransportation) TJ0 -1.3167 TD0.132 Tw[(Security)56(Administration, with names fed to it) TJT*0.016 pursuant to see new

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.

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 SIGNATURE: THE CURRENT RATE SECURITY COMPLEX

In Dwight Eisenhower’s farewell address at the end of his presidency in 1961, he warned themindu647ste6(9/1)40(1.

The US-VISIT program (see p.) is another goldmine for the corporate sector. Congress

cards with chips and biometrics to Macau, ID cards to Bosnia-Herzegovina and Italy, and visas to Norway.²⁴⁰ In 2002, the France-based

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

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

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

extraterritorial detention camps and centres on

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

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

Adriens en was afgedrukt in me.0 Ta confes0 If pabel0 T 25ther memorande0.183 Twys wereview0 Tonain a

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

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,

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

h) New License for Brutal Regimes

Malaysian students detained without trial in Karachi, Pakistan, in September 2003, the Malaysian government remained silent rather than protest the detention.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,

before the event.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. 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

possible, but in the current political climate,

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.

Concerns about the surveillance agenda are also filtering into democratic bodies. Multi

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

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

¹²⁰ Michael Sniffen, “Controversial Terror Research Lives On”,
Washington Post

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), n 70i07 http://europa.eu.int/eur-lex/en/com/cnc/2004/com2004_0590en01.pdf [December 23, 2004].

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

²²² ACLU, *et al. v. National Security Agency*, *supra* note 77, pp. 726-28.

²²³ Adam Mayle and Alex Knott, *Outsourcing Big Brother: Office of Total Information Awareness Relies on Private Sector*

²⁴⁸ Stephen Grey, *supra* note 153.

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

²⁵⁰ Stephen Grey, *supra*

February 7, 2002. <http://hrw>

A01. [Priest and Gellman . See also, Dozens of Secret Jails,

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

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>

International Campaign Against Mass Surveillance

