Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the U.S. and Europe

Gus Hosein

December 13, 2005

Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the U.S. and Europe

We are not surprised to see the introduction of new powers of the State in response to terrorism. We are also not surprised when we are informed that the new powers are absolutely necessary for the maintenance of security and our open societies. We also frequently see Governments implementing new powers whilst arguing that they are merely modelling the actions of other countries.

While none of these dynamics are surprising we remain blinded by the politics of anti-terror policy. We are missing much by focusing merely upon the dynamics in a single country, often a disproportionate amount of attention on the United States, and by focusing on merely one aspect and point in time of an entire policy regime whilst missing out on the broader public deliberations.

Our first blind spot is our lack of attention to the divergences in laws from country to country. Though we frequently see governments modelling from each other's policies, like the UK Government refer to France's ID cards or deportation powers as supporting evidence for its own cause for greater powers, we don't often question the differences in the legal systems and political landscape. Also, if the Government of Italy argues that a policy is absolutely essential to the combating of terrorism why doesn't the U.S. or Germany have a similar law? It is not so simple as to explain away this difference by saying that these other countries are lacking resolve.

Another blind spot in the war on terror is generated by the focus on the United States. There is a great deal of global public attention on the variety of powers introduced by the U.S. Congress in the months and years after September 11, 2001. This global public attention is usually at the cost of national attention to local laws. We point easily to the USA-PATRIOT Act and the new border policies in the U.S. but we don't know of similar and more expansive initiatives in the EU.

A third blind spot is generated by the lack of long-term attention to the legislative and legal processes. Indeed many countries introduced extraordinary laws and policies. Over the years, however, these laws may come to be questioned in parliaments, the media, the courts, and in the public sphere. Some have in fact been seriously amended, found unconstitutional, while others have been enhanced.

In this report we investigate these blind-spots in detail. We will conduct a comparative analysis of a variety of powers introduced by the United States and the European Union.

Through this investigation we may find evidence that will aid in reducing the risk that policies infringe upon civil liberties unnecessarily.

All the powers that we cover in this report will have significant implications for the Open Society. Here we look at powers of communications surveillance and regulations affecting freedom of movement through the development of new internal, travel, and border surveillance systems. Generalised surveillance systems may be used to limit individual freedom and in particular could be applied in such a way to limit our ability to access and impart information, organise and assemble, and to live free from arbitrary interference. These rights are fundamental to the Open Society.

Though the Open Society is in peril, there is much to be hopeful for. This report finds that in the U.S. there is a continuing debate surrounding anti-terrorism policies. However the situation in Europe is far more bleak, as the policy processes in the EU appear to be more opaque. We draw particular attention to the expansive regimes being established in the EU, as they go well beyond standards set in the U.S. The EU is also failing to learn from policy failures that have arisen elsewhere and is moving to implement policies that even the U.S. has abandoned. The EU is ignoring the need for adequate safeguards, authorisation and oversight processes in ways that would not be even entertained in the U.S. And the EU suffers from a remarkable lack of debate, in part due to a weaker civil society, a lack of media attention, and weak institutional procedures with an over-powerful lawmaking institution, i.e. the European Council.

Policy	U.S.	EU
Access to Communications Data, i.e. telephone and internet logs and location of mobile phone calls.	Judicial authorisation required except in cases involving terrorism.	No judicial orders required and permitted for all investigations.
	Debate: Legislation proposing safeguards, years of congressional debate, high media awareness, local campaigns, court cases.	Debate: European Council is coercing European Parliament so as to avoid discussion on this matter.
Retention of Communications Transactions Data.	No policy.	Communications industry must retain data on all transactions for between 6 months and up to four years.
	Debate: None.	Debate: European Council is calling on the European Parliament to agree to Council demands or else the Parliament will be removed from the process.

Policy	U.S.	EU
Data profiling and data mining.	Various projects have been dropped and funding cut.	Projects in progress.
	Debate: Intense media and NGO activity, Congressional scrutiny, governmental reports.	Debate: None.
Access to Passenger reservation files.	Access to data held by Foreign carriers only, for combating terrorism and serious crime.	Plans to access from all carriers for any purpose.
	Debate: Little debate on access to foreign carriers; larger debate on access to travel profiles and data stores of domestic travel with NGO activity, media attention and court cases.	Debate: None.
Biometric registration.	Foreigners only (fingerprints and face scans). Passport holders will be face-scanned.	All Europeans will be face-scanned and fingerprinted at a minimum.
	Debate: Intense debate in U.S. with extensive consultation.	Debate: Limited. Council called on Parliament to agree to demands or else Parliament would be removed from the process.

In each case the EU is implementing surveillance powers well beyond those in U.S., and with far less openness and debate over these measures. The only area in which the U.S. matched the EU for closed discussion and lack of public debate is on matters that affect non-U.S. citizens and non-U.S. companies. This is particularly the case over the use of technology at borders. In the U.S. there was little debate about the installation of the US-VISIT system; and in Europe, as with most other surveillance policies, there are few discussions on the direction of these policies and little debate.

This report concludes that the two policy blocs can learn more from each other than how to expand powers,. They may also share in some lessons learned from the mistakes in each others' processes and policies. Perhaps this could lead to renewed attention to safeguards and protections from abuse.

About this Report

This report was written by Dr. Gus Hosein, a Senior Fellow at Privacy International and a Visiting Fellow in the Department of Information Systems at the London School of

Economics and Political Science. The research was funded by the Open Society Institute's Information Programme and the Open Society Justice Initiative's programme on Freedom of Information/Expression, as part of Privacy International's *Terrorism and the Open Society* programme. The author would like to thank the following people for their consultative advice: David Banisar, Tony Bunyan, Simon Davies, Chris Pounder, Barry Steinhardt, Peter Swire, and Rosemary Walsh.

Table of Contents

Terrorism Policies, Civil Liberties, and Individual Autonomy

Most civil liberties are being curtailed in the era of combating terrorism. It is possible to focus an analysis of this curtailment just on freedom of expression. Many countries have cracked down on incitement to terror, some are considering regulating the glorification of terrorism, and have regulated protest activities and religious practices. Increasingly individuals are stopped and searched at protest marches and public events, websites are pulled down, journalists are under investigation, and rules arise to regulate blasphemy and hate speech.[1]

Certainly free expression is under duress. However, it is important to also focus on other civil liberties in order to better understand the dynamics at play. We need to look at the conditions that give support to the practice of free expression, including the principles on good governance and promotion of individual autonomy.

Civil liberties may be considered as a set of principles enumerated within conventions and constitutions. Often in the face of terrorism these enumerated lists are placed lower on the agenda than the preservation of security of the state. Of course this is not new. This is the fundamental conflict of all political systems. This led some governments to separate the executive, the legislature, and the judiciary. Each are given differing responsibilities to ensure good governance and the preservation of the system of government. Those responsibilities are never more important than at times such as ours.

There is more to civil liberties than lists and principles. Civil liberties establish conditions for good governance and for the protection of the individual's autonomy. When the Council of Europe countries agreed to the European Convention on Human Rights in 1950 they also acknowledged that some rights are not absolute. But in curtailing the rights that may be limited, the ECHR requires that interferences with these rights must be necessary in a democratic society. The European Court of Human Rights in turn established that powers must have a legal basis, that there is a pressing social need, the interference must be proportionate and legitimate, individuals must have remedies and powers must be reasonable; among a number of other conditions. These 'conditions' can be considered as necessary to good governance and responsible legislation.

With all the changes in civil liberties since the rise of terrorism on the policy agenda we are threatening the principle of the Open Society. That is the Open Society is a society that

[1] For an analysis of some of the rules on free expression, see "Open Society and the Internet: Future Prospects and Aspirations" by Gus Hosein, in The Media Freedom Internet Cookbook, pages 242-263, published by the Organisation for Security and Cooperation in Europe, Vienna.

believes that laws must be questioned, authorities scrutinised, and that governments are not perfect. That a government claims that a policy is necessary does not make it true. Other institutions in society exist to call these policies into question. These other institutions are just as much a part of the protective guard of the open society as the executive arm of government. Together they ensure that policies and laws are well-formed, reasonable, proportionate, and all the other conditions that are provided for by civil liberties.

To understand the ramifications of terrorism policy on the Open Society we may look at the changes in surveillance of communications and movement. Each have links with free expression. Communications surveillance chills free expression and hampers the rights of individuals to access and impart information. New systems that monitor our movement and decide our eligibility to travel and pass through borders hit directly at our autonomy and our freedom of assembly rights. When non-governmental organisations are placed under investigation, or no-fly lists prevent the travel of protestors we understand that these actions impinge on freedom of expression; but these policies themselves are also threats to the Open Society.

By looking at the dynamics of anti-terrorism policy on the larger spectrum of civil liberties we are able to understand better the breadth of changes in our midst. Most importantly we will be able to see the divergences between various governments' strategies even as they all argue that their proposed policies are absolutely essential to combating terrorism. Understanding these divergences will permit us to question the bases for which governments are monopolising the political process.

Protecting the Open Society is not merely a security exercise. This report will show that what is most threatened is the process through which policy is introduced, decided, and questioned. Recently the Commission established to investigate the attacks on September 11 2001, i.e. the '9/11 Commission', admonished the U.S. Congress for not doing enough to enforce its recommendations that protect civil liberties even while Congress acted with fervour to implement headline-making powers for the Federal Government.[2] While it is possible to argue that Congress may have been sleeping while on the watch for an over-active executive, it is not alone as many Parliaments have been inactive in protecting civil liberties. Policies are rushed through and sometimes laundered through international institutions without adequate oversight and independence from the will of governments. In the U.S. the landscape is not so bleak however as other institutions have stepped in to act

[2] "9/11 Panel Says Congress and White House are Failing to Act", Philip Shenon, The New York Times, October 19, 2005. To be fair, the FBI was also criticised for failing to share information with other government departments and failing on internal changes such as the implementation of a new computer system.

as opposing forces. The great worry about Europe is that there are few who have stepped in to replace the silent and silenced parliaments, while the institutions such as the media and non-governmental organisations pay scant attention to the worrying developments.

What the U.S. has Done

Around the world the U.S. is regarded as the *enfant terrible* for its policies on terrorism. It appears that almost everyone on the planet has an opinion on the USA-PATRIOT Act and other related policies that emerged after September 11, 2001. To many around the world the U.S. is the epitome of the radical transformation of a society from an open society to a security state. Before such rash conclusions are drawn it is better for us to actually look in detail at some of the policy changes that were introduced.

Much changed in the U.S. after September 11, but the changes are not necessarily permanent. Of course there is much that will not be included in this overview and analysis. The Bush Administration and the U.S. Congress introduced a raft of new policies including the power of detention without trial, military tribunals, Guantanamo Bay prison facilities, conditions for detaining 'material witnesses', alterations to attorney-client privileges, a re-organisation of government through the establishment of a new agency and cabinet position for Homeland Security. These are all worthy of scrutiny as well, as have been reported elsewhere. Instead we focus on select policies below that relate to surveillance and individual autonomy.

Setting the Landscape: The USA-PATRIOT Act

The USA-PATRIOT Act is perhaps the most well-known piece of legislation in the world. The 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001' is the result of a flurry of legislative initiatives in response to the hijackings and attacks on New York and the Pentagon. Eventually a number of bills were combined together including the Bush Administration's 'Anti-Terrorism Act', the House's bill the PATRIOT Act, and the Senate's bill the USA Act, to create the USA-PATRIOT Act (hereon 'the Patriot Act').

As these bills were combined some of the more radical components in each were cut. However some components were drafted by the Department of Justice behind closed doors and were left unchanged. It passed in the House on a vote of 357-66. When it reached the Senate a number of components were given a four-year expiration date, and was then approved 98-1.

Then-Attorney General John Ashcroft promised that the law would be used to be tough on terrorism.

> "Robert Kennedy's Justice Department, it is said, would arrest mobsters for 'spitting on the sidewalk' if it would help in the battle against organized crime. It has been and will be the policy of this Department of Justice to use the same aggressive arrest and detention tactics in the war

> on terror."[3]

On signing the bill on October 26, 2001, President Bush noted the breadth of the law:

> "This legislation gives law enforcement officials better tools to put an end to financial counterfeiting, smuggling and money-laundering. Secondly, it gives intelligence operations and criminal operations the chance to operate not on separate tracks, but to share vital information so necessary to disrupt a terrorist attack before it occurs. As of today, we're changing the laws governing information-sharing."[4]

The Patriot Act is a large piece of legislation with many components: it is over 300-pages long and amends over 15 different statutes.[5] It begins on a high note by condemning discrimination against Arab and Muslim Americans, and then moves on quickly. It increased funding for a number of agencies and departments. Enhanced surveillance powers were introduced, as well as measures on combating money laundering and terrorism financing, border control mechanisms and systems, detention powers against suspected terrorists, requirements for international biometric identity documents, the collection of DNA from terrorists and violent offenders, disclosure of educational records, aid to victims of terrorism, increased data-sharing for critical infrastructure protection, changes to intelligence collection on foreigners, and a new definition of terrorism and new associated crimes.

The surveillance and data-sharing components of the bill are numerous and often-expansive. The most contentious aspects of the bill that are relevant to this report are:

- the expansion of communications surveillance powers including broad warrants for interception of communications and access to communications traffic data;
- an increased use of subpoenas and gag orders preventing the disclosure of the fact that a subpoena was served;
- access to passenger travel data;
- the creation of biometric passports; and
- the establishment of an entry-and-exit border system.

A general change in government power also occurred with increased data-sharing between law enforcement agencies and intelligence agencies, and the broadening of the use of national security powers. Some of these issues were further changed in later legislation and policy shifts.

---

[3] Ashcroft at a speech to the U.S. Conference of Mayors in Washington, reported on CNN, "Bush to sign new anti-terrorism bill", Terry Frieden, CNN, October 26, 2001.
[4] "President Signs Anti-Terrorism Bill: Remarks by the President at Signing of the Patriot Act", The White House, October 26, 2001.
[5] EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities (Oct 31, 2001).

Monitoring Travel and Movement

The Patriot Act is not the only policy through which the U.S. Government established new powers and systems. Many policies were introduced, new systems trialled, and their achievements heralded and derided. A subset are addressed below.

Logging of Movement: Access to passenger data

The Aviation and Transportation Security Act 2001 is the lesser-known law passed in the aftermath of September 11, 2001. This law instituted a requirement that foreign carriers "shall make passenger name record information available to the Customs Service upon request", and provided for this information to be shared with other agencies outside of the Transportation Security Administration (TSA). The availability of this information was deemed necessary for purposes of "ensuring aviation safety and protecting national security." It is important to note that U.S. carriers would not need to comply with this requirement; only foreign carriers.[6] If domestic travel records were included[7] the collection of this data is tantamount to a tracking of all air travel within, to and from the U.S.

This transportation data, or 'PNR', consists of all the details of reservations, payment, and preferences:[8]

- Identification data: name, first name, date of birth, telephone number;
- Transactional data: the dates of reservations, the travel agent where appropriate, the information displayed on the ticket, the itinerary;
- Financial data: credit card number, expiry date, invoicing address etc.;
- Flight information: flight number, seat number, etc.;
- Earlier PNR: may include not only journeys completed in the past but also religious or ethnic information (choice of meal etc.), affiliation to any particular group, data relating to the place of residence or means of contacting an individual (e-mail address, details of a friend, place of work etc.), medical data (any medical assistance required, oxygen, problems relating to sight, hearing or mobility or any other problem which must be made known to ensure a satisfactory flight) and other data linked, for example, with frequent flyer programs.

Under the policy, the data is retained for vast periods of time: first proposed to be 50 years, though in one agreement made with the European Commission the TSA was reduced the retention period to 3.5 years. Originally proposed to be used for general law enforcement

[6] Instead, domestic carriers were approached to voluntarily disclose vast data stores in relation to investigating the September 2001 attacks and to test out data mining systems (see below).
[7] as is currently being planned.
[8] Adapted from Article 29 Working Party. "Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States." Brussels: European Commission, 24 October, 2002.

purposes it was eventually limited, after much debate, to combating terrorism and serious organised crime.[9] The data would be used to better identify problem passengers through watch-list verification or mining the data for intelligence purposes.

Registration of Foreigners

There is a further purpose for accessing this data: border management. The U.S. has led the world with enhancements to border controls through the use of technologies for immigrant registration. In 1996 Congress called on the Attorney General to develop an automated entry and exit monitoring system for foreigners. The Patriot Act suggested the use of biometrics. The Enhanced Border Security and Visa Entry Reform Act 2002 called for the integration of this data with other databases.

The development of a system for automated surveillance of visitors to the U.S. began immediately after September 11, 2001. After the terrorist attacks, the Immigration Services identified 7602 individuals who shared similar characteristics to the 19 hijackers. And over time, law enforcement officials interviewed 3,000 Muslim and Arab immigrants in the U.S. The list contained many duplicate names and data entry errors, and the practice was later considered to have an adverse effect on relationships with these communities.[10]

Then followed the 'Special Registration Procedures for Certain Non-immigrants'. This involved the forced registration, interviewing and fingerprinting of individuals. The programme originally started with fingerprinting and interviewing of citizens or nationals of Iran, Iraq, Libya, Sudan and Syria, but also "any other non-immigrant identified by INS officers at airports, seaports and land ports of entry", based on criteria designated by the Secretary of Homeland Security.[11] The programme was later extended to include individuals from Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates and Yemen.

The National Security Entry-Exit Registration System followed. Ironically, registration was justified on the grounds that the European authorities have registered visitors for some years. According to the Justice Department:

> "Our European allies have had similar registration systems in place for decades and know the value of ensuring that foreign visitors are doing what they said they would do and living where they said they would live.

[9] See Privacy International's report "Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection", February 2004.
[10] "HOMELAND SECURITY: Justice Department's Project to Interview Aliens after September 11, 2001", General Accounting Office, GAO-03-459, April 2003.
[11] Title 8 of Code of Federal Regulations (8CFR). Part 264.1.f.

> The NSEERS system takes the European model and combines it with a modern intranet system so that files may be updated in real time at any INS office in the country."[12]

Under NSEERS, these individuals would be 'fingerprinted and processed'. It was not limited to 'terrorist nations', however. According to the then-Attorney General, John Ashcroft:

> "So far, [Immigration and Naturalization Services] has fingerprinted and registered individuals from 112 different countries. From the Baltic to the Balkans and from the Cape of Good Hope to the Rock of Gibraltar, visitors who may present elevated national security concerns will be included. No country is exempt. In the war against terrorism, we cannot afford to have tunnel vision".[13]

In April 2003 NSEERS was folded into the U.S. Visitor & Immigration Status Indication Technology System (US-VISIT) programme. Although the US-VISIT programme would end the domestic special registration, it would register all visa-holders to the U.S., and was later extended to all visitors to the U.S.

This data system is to be used for a plethora of purposes. These include national security, law enforcement, immigration control, and "other mission-related functions and to provide associated management reporting, planning and analysis."[14] This personal information will be retained for 75 to 100 years and shared across government departments.[15]

Registration of Citizens: Passport and ID

Collecting travel patterns and border movements also requires the collection of more information about individuals and their identifying marks, including data on Americans. The Patriot Act required that the President certify a biometric technology standard for use in identifying aliens seeking admission into the U.S., within two years. The schedule for its implementation was accelerated by another piece of legislation, again the Enhanced Border Security and Visa Entry Reform Act 2002. That policy placed a requirement upon other countries to implement a biometric passport.

> "By October 26, 2004, in order for a country to remain eligible for participation in the visa waiver program its government must certify that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and which incorporate biometric and authentication identifiers that satisfy the standards of the International

[12] "Attorney General's Remarks on the Implementation of NSEERS", Department of Justice, Niagara Falls, New York: November 7, 2002.
[13] ibid.
[14] Federal Register, Department of Homeland Security, [DHS/ICE/CB/CIS001] Privacy Act of 1974; System of Records, Federal Register, Volume 68 Number 239. December 12, 2003.
[15] For an analysis of this datasharing regime, please see Privacy International's assessment of the US-VISIT System at http://www.privacyinternational.org/issues/terrorism/rpt/dangers_of_visit.pdf.

Civil Aviation Organization (ICAO)."[16]

After two years the ICAO was finally able to establish a biometric standard: face recognition. As a result, all future ICAO-compliant passports must contain a digital photograph. However the ICAO also permitted countries to include other biometrics including fingerprints and iris-scans. In October 2005 the U.S. Department of State announced its own biometric passport programme, established to adhere to international standards (that it created) involving facial recognition. This is despite a consultation process where over 90% of the responses opposed the changes to the passport on grounds of privacy and technological challenges; although some changes were achieved to minimise data disclosure.

Unlike in Europe, a small proportion of Americans hold passports. As part of the 9/11 Commission's investigation into the events and intelligence failures that led to the September 11 attacks in New York and Washington, the Commission recommended the standardisation of States' driving licences. In February 2005 the House of Representatives approved H.R. 418, the REAL ID Act. It became law in May 2005 following unanimous approval in the Senate after it had been attached to a funding bill for the military operations in Iraq, and Tsunami relief. Up until this point, the legislation had encountered significant opposition from politicians and groups from across the political spectrum. The White House supported the policy, as it will "strengthen the ability of the United States to protect against terrorist entry into and activities within the United States."[17]

The law requires States to deny driving licenses to undocumented immigrants: this requirement is seen as moving the license into the realm of a national ID card. Temporary residents will only get a license that is valid until their authorised period of stay expires. For all other non-citizens, licences will be valid for only one year.

The database of licences and associated data that is generated under this regime will be shared across states, and with Mexico and Canada. The law specifies information to be held in the database, including name, date of birth, gender, digital photograph, signature, and address.

The law also calls on the Secretary of Homeland Security to "prescribe one or more design formats" for the licenses. This could lead to the use of identifying radio tags in licences or

[16] Enhanced Border Security and Visa Entry Reform Act of 2002 - ALDAC No. 1, R 152341Z MAY 02, FM SECSTATE WASHDC TO ALL DIPLOMATIC AND CONSULAR POSTS SPECIAL EMBASSY PROGRAM, AMEMBASSY KABUL, AMEMBASSY DUSHANBE UNCLAS STATE 093239, VISAS, E.O. 12958: N/A, TAGS: CVIS.

[17] "Statement of Administration Policy on H.R. 418 – REAL ID Act of 2005", Executive Office of the President, February 9, 2005.

possibly the use of biometrics such as fingerprints.

The general response to the Act is one of widespread concern. There are reports of a number of plans to appeal to the courts on the matter. For instance, the National Governors Association threatened lawsuits on the grounds that it will cost States up to $700 million to comply with the law. The Mexican Government is prepared to lodge a diplomatic complaint regarding the law, referring to it as "negative, inconvenient and obstructionist." In a sense, the debate on this policy is only now beginning.

Data Mining and Profiling

Frequently debate on a policy only begins after the policy has been decided. In its earliest responses to the terrorist attacks in 2001, the U.S. Government considered the power of data mining to combat terrorism. There was no enabling legislation, in-depth policy analysis, or debate over the use of technology to weed out terrorists until programmes were already in their development stage.

Data mining is interpreted in a variety of ways, but according to the U.S. Government Accountability Office (GAO), it is the

> "the application of database technology and techniques such as statistical analysis and modelling to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results."[18]

The GAO reports that 128 federal departments are using data mining for a variety of purposes, ranging from improving service or performance to analyzing and detecting terrorist patterns and activities. The latter systems generated significant controversy.

Total Information Awareness

The most controversial proposal was the Total Information Awareness program, run by the Defense Advanced Research Projects (DARPA) at the Department of Defense. According to its early system description documents[19] the system would provide "a true end-to-end capability for analysts and decision-makers", that will "visually tie all levels of the system together, generating insight from architectural patterns, and facilitating drill-down to understand underlying rationale." Over its 150 pages the System Description Document describes a massive system that is able to scan, compile, and process personal data of all people within and outside of the U.S. in order to establish patterns, generate hypotheses, reporting and alerting, and to detect facts and events.

---

[18] General Accounting Office, DATA MINING: Federal Efforts Cover a Wide Range of Uses. 2004.
[19] Mack, G., B. Bebee, and G. Wenzel, Total Information Awareness Program System Description Document. 2002, Information Awareness Office.

U.S. Undersecretary for Defense Pete Aldridge was called on to describe the application of this data mining system.

> "The war on terror and the tracking of potential terrorists and terrorist acts require that we search for clues of such activities in a mass of data. It's kind of a signal-to-noise ratio. What are they doing in all these things that are going on around the world? And we decided that new capabilities and new technologies are required to accomplish that task. (...) The purpose of TIA would be to determine the feasibility of searching vast quantities of data to determine links and patterns indicative of terrorist activities."[20]

He went on to describe a system that include voice recognition, identify connections between individuals and transactions, linking together driver's licenses, gun purchases, airlines tickets, and visas.

When asked regarding any concerns that may arise due to privacy and spying, Aldridge noted:

> "First of all, we are developing the technology of a system that could be used by the law enforcement officials, if they choose to do so. It is a technology that we're developing. We are not using this for this purpose. It is technology. Once that technology is transported over to the law enforcement agency, they will use the same process they do today; they protect the individual's identity. We'll have to operate under the same legal conditions as we do today that protects individuals' privacy when this is operated by the law enforcement agency."[21]

The response from media organisations was significantly different. The Washington Post editorial on the issue questioned the government's benign view of the technology.

> "For however revolutionary and innovative it may be, this is not neutral technology, and the potential for abuse is enormous. If information that once took five people a week to find will now take one person 15 minutes to find, then instant -- and instantly updatable -- computer dossiers on everyone really do cease to be science fiction. If computers can learn to identify a person through a video camera, then constant surveillance of society becomes possible, too. Because the legal system designed to protect privacy has yet to catch up with this technology, Congress needs to take a direct interest in this project, and the defense secretary should appoint an outside committee to oversee it before it proceeds."[22]

Similarly the New York Times contested the 'technology is neutral' approach taken by the DARPA group and described TIA differently.

---

[20] Department of Defence, Defense Department Briefing Transcript. 2002: Washington.
[21] ibid.
[22] Washington Post Editorial Page, Total Information Awareness, in Washington Post. 2002. p. A20.

> "Total Information Awareness, or T.I.A., aims to use the vast networking powers of the computer to "mine" huge amounts of information about people and thus help investigative agencies identify potential terrorists and anticipate terrorist activities. All the transactions of everyday life: credit card purchases, travel and telephone records, even Internet traffic like e-mail would be grist for the electronic mill."[23]

A number of policy experts in non-governmental organizations weighed in over the following months, with initiatives often led by the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center, and the Center for Democracy and Technology. Through a number of conferences, campaigns, press releases, and lobbying, these NGOs played important roles in painting a picture of the dark role of TIA within American society.

Over time this mass of action, not always collectively organized, led to the relative demise of the program. The U.S. Congress passed a provision (near unanimous) preventing TIA from using personal data on American citizens. Then it called for a report from the Department of Defense on the program's costs, goals, impact on civil liberties and prospects for success against terrorists. The ACLU called on the Pentagon to address the following issues within the report:

- How Americans can remain free when their every transaction is opened up to potential government scrutiny;
- How the system will be effective in the face of a false positive rate that even under the most optimistic assumptions will reach crippling levels, and other problems;
- The TIA's technological capabilities, including whether it could work with one giant, centralized database, and whether there would be any limit to the number of databases to which it could connect;
- Whether the system will be able to do true data-mining, or only more limited "query-based" searches;
- Why it makes a difference, as the government has been suggesting, that the TIA database would be distributed rather than centralized;
- How the bedrock American principle of "individualized suspicion" will be maintained in the face of a system designed to guess about who might be a suspect; and,
- How TIA is likely to evolve over time given the well-established historical tendency

[23] New York Times Editorial, A Snooper's Dream, in The New York Times. 2002.

for such programs to expand once they are established.[24]

The Department of Defense followed up with a new name for the project and some mechanisms to restrict privacy invasion. TIA was renamed 'Terrorism Information Awareness' to avoid the connotation of mining through citizens' personal information. The response from the NGOs was cold, and the references to George Orwell's 1984 only amplified. According to Barry Steinhardt at the ACLU,

> "It is grimly appropriate that this Orwellian program is being sold to us in such an Orwellian manner. The government can't expect us to forget everything they've said before about this program just by changing its name."[25]

A few months later, in July 2003, Congress voted to cut funding from the program.

Passenger Profiling: CAPPS II

In response to the breaches of airport security that took place on September 11, 2001, the U.S. Government entrusted the Transportation Security Administration (TSA) to develop a technological means to prevent future terrorists and serious criminals from escaping detection. On top of the raft of new security scanners and training for staff, the TSA decided to innovate by introducing a successor to its Computer Assisted Passenger Profiling System (CAPPS) by developing a more sophisticated Computer Assisted Passenger Pre-Screening System (CAPPS II).

CAPPS I identified passengers for enhanced screening before they boarded planes. This first generation profiling system was considered to have failed on September 11, 2001 so work began on the development CAPPS II. According to the TSA in testimony to Congress:

> "The purpose of CAPPS II is to identify foreign terrorists and those with links to foreign terrorists that pose a threat to civil aviation security. CAPPS II will allow TSA make more efficient use of screener resources by using dynamic intelligence information to select passengers for enhanced screening."[26]

The TSA argued that CAPPS II would be more efficient than CAPPS I (which stopped 15% of travellers):

> "Essentially, CAPPS II will be a passive system that produces a general

[24] American Civil Liberties Union, New ACLU Report Specifies Questions Needing Answers, in ACLU Press Release, May 16, 2003.
[25] American Civil Liberties Union, Pentagon Releases Report on Cyber-Surveillance System's Privacy Threat; Right-Left Groups Urge Continued Oversight, in ACLU Press Release, May 20, 2003.
[26] Loy, J.M., Statement of Admiral James M. Loy, Administrator, Transportation Security Administration, before Committee on Government Reform, U.S. House of Representatives, May 6, 2003.

> indication of the level of terrorist risk each airline passenger might post to civil aviation security. Airlines will ask passengers for specific reservation information that will include a passenger's full name, plus other identifiers including date of birth, home address, and home phone number. Passengers will not be asked to provide social security numbers, and TSA will not look at credit worthiness. The CAPPS process will then authenticate each passenger's identity through publicly and commercially available databases. Once a passenger's identity is authenticated and the passenger's information is run against terrorist or other appropriate Federal government systems, an aggregate numerical threat score will be generated that TSA will use to determine which passengers should proceed through the ordinary screening process and which passengers should be asked to submit to a somewhat more thorough screening process."

The TSA had learned from the TIA policy disaster and was careful to denote the system as a pre-screening system, that focused only on terrorists:

> "CAPPS II is a passenger-screening tool only. It will not ingest or store large quantities of data. Very importantly, CAPPS II is not data mining in that it will not explore databases to extract information to identify patterns of behavior among travelers."

CAPPS II would gain access to vast data stores of PNR from the reservation systems of airlines and mine this data to identify problem passengers.

The promises of minimal intrusions into the private lives of travellers did not prevent controversy from arising. Media organisations painted bleak images of the system; for instance the New York Times called CAPPS II "a highly intrusive surveillance program" that "raises serious privacy and due process concerns".[27] It was reported that the system would compare personal information against criminal records and intelligence information. It was also reported that both liberal and conservative groups opposed the initiative.[28] Some NGOs saw it as a tool that could never actually work, and would identify innocents as potential terrorists.[29] Others predicted that it was more of a law enforcement tool, and had less to do with combating terrorists. A number of security experts doubted whether the system could be built to do what it intended.

Amidst these concerns regarding civil liberties and feasibility, the system was shelved in July 2004 in a public statement by the Secretary of Homeland Security, as he even mimicked a stab in the heart when asked 'how dead was the project?'. The Department of Homeland Security argued that the project failed because of privacy concerns, and eventually

[27] New York Times Editorial, The New Airport Profiling, in The New York Times. 2003.
[28] "Fliers to be Rated for Risk Level", S.K. Goo, Washington Post, September 9, 2003, p. A01.
[29] American Civil Liberties Union, Testimony of Barry Steinhardt before the House Government Reform Subcommittee, May 20, 2003.

conceded that technological challenges were also largely to blame.[30]

It has since then been replaced with a relatively simplified watch-list program, Secure Flight, that does not query external databases, thus reducing the data-mining component. Even this system is failing under public pressure and design constraints.

Private Sector Profiling: MATRIX

Our political system is designed to foster debate and deliberation on public policy issues. When the policies are removed from the public sphere matters become more complex. Data mining and profiling may be done by the private sector, away from parliaments and oversight mechanisms, and away from the laws that restrict the processing of personal information by government agencies. The private sector operates under a very different regulatory regime with few of these restrictions.

These differences between the public and private sectors were the guiding principles behind the MATRIX system. The Multistate Anti-Terrorism Information Exchange (MATRIX) project, established by a Seisint, a Florida-based company, proposed to do the data mining for both the Federal and State Governments. According to the project documentation:

> "[the MATRIX] project leverages proven technology to assist criminal investigations by implementing factual data analysis from existing data sources and integrating disparate data from many types of Web-enabled storage systems. This technology helps to identify, develop, and analyze terrorist activity and other crimes for investigative leads. Information accessible includes criminal history records, driver's license data, vehicle registration records, and incarceration/corrections records, including digitized photographs, with significant amounts of public data records. This capability will save countless investigative hours and drastically improve the opportunity to successfully resolve investigations. The ultimate goal is to expand this capability to all states."[31]

This information is then given to the police when they look up an individual. This is aimed to 'fill in the gaps', according to its developers.

> "The MATRIX pilot project utilizes the Factual Analysis Criminal Threat Solution (FACTS) application that provides law enforcement a technological, investigative tool allowing query-based searches of available state and public records in the data reference repository. Using FACTS, an investigator can conduct a query using incomplete information, such as a portion of a vehicle license number. FACTS will search the system and assemble information matching the partial

[30] "U.S. rethinks airline passenger screening plan", L. Bernardini, CNN, July 15, 2004.
[31] MATRIX, "Matrix defined", 2004, from the Matrix website (was at http://www.matrix-at.org) but has been discontinued.

description."[32]

Again, the media, politicians, and non-governmental organizations voiced displeasure with the system. The ACLU gained access to Federal and State Government files on MATRIX to investigate and report on its full dynamics.

The private contractor behind MATRIX, Seisint Inc, created this data mining tool by utilizing the Terrorist Handbook (apparently a terrorist's manual on penetrating and living in American society), as well as the following data:

- Age & Gender;
- What they did with their driver's license;
- Either pilots or associations to pilots;
- Proximity to "Dirty" addresses/phone numbers;
- Investigational Data;
- How they shipped, How they received;
- Social Security Number Anomalies;
- Credit Histories; and
- Ethnicity.

Seisint compiled a list of 120,000 names that merited further investigation and shared that list with the Immigration and Nationalization Service, the FBI, the Secret Service.[33]

Under accusations that this was 'Big Brother's little helper', and worries about the inaccuracy of information that is then mined to provide even more faulty results, individual States began pulling out of the system. When MATRIX shut down in March 2005 only two States remained.

Data mining is by no means a dead policy issue in the U.S. Alternative solutions are being sought. The current Secretary of Homeland Security, Michael Chertoff, recognizes that the TIA solution received a chilly public response. In turn he is reported to have stated at a conference that instead of Government performing such tasks, "[m]aybe we can create a non-profit and track people's activities, and an algorithm could red-flag individuals. Then, the nonprofits could give us the names".[34] This policy has not yet moved forward, and led to statements from Homeland Security officials that the Secretary's words were mere speculation.

Surveillance of Transactions

Over the years a number of the above policies have been scrutinised by media organisations, activists, policy experts, and local governments. This is particularly true of the Patriot Act.

[32] MATRIX, "What is FACTS?", 2004, from the Matrix website.
[33] American Civil Liberties Union, Letter to the Chief Privacy Officer of the Department of Homeland Security, dated May 19, 2004. 2004: Washington, D.C.
[34] Gorman, S., DHS chief floats idea of collecting private citizens' information, in GovExec.com. 2005.

More than 400 local communities and seven states have passed resolutions to reform the Patriot Act. Coalitions opposing the bill have been forged drawing together those with diverse views of politics.[35] There was even international concern: Canadian provincial and federal privacy commissioners were called on to investigate what happens to medical data on Canadians that are maintained by U.S. companies for fear that the data could be accessed easily by U.S. officials.[36]

The scrutiny grew to such a point that the Attorney General performed a cross-country road-show and launched a website[37] to defend the Act and to generate support in time for the renewal of the sections that were due to expire under sunset provisions. President Bush was forced to enter to the fray and express support for the law's renewal and expansion:

> "Some politicians in Washington act as if the threat to America will also expire on that schedule. Yet, we have seen what the terrorists intend for us, in deadly attacks from Bali to Mombassa to Madrid. And we will not forget the lessons of September the 11th. To abandon the Patriot Act would deprive law enforcement and intelligence officers of needed tools in the war on terror, and demonstrate wilful blindness to a continuing threat."[38]

It later even became an election issue.[39]

Some members of Congress drafted bills to undo the more contentious aspects of the Patriot Act even before some provisions sunsetted. The "Security and Freedom Ensured Act of 2003" was introduced into the Senate to amend the sections on 'sneak and peek', communications and computer surveillance, and access to business records.[40] The "Civil Liberties Restoration Act" was also introduced into the Senate to 'restore' free expression rights, to 'provide' due process, to terminate immigrant registration programmes, reporting on data mining activities, and erasing the gag orders on searches and increasing judicial oversight.[41] A number of other legislative initiatives were introduced to cut off federal funding for specific types of searches and programmes.

The increasing opposition to the Patriot Act continues to generate concern in the Bush Administration. When the Senate introduced a number of proposed restrictions to the

---

[35] See for instance, http://www.checksbalances.org, drawing together conservative political thinkers with liberal non-governmental organisations.
[36] "B.C. touts privacy shield that offers protection from U.S. Patriot Act", Dirk Meissner, Canadian Press, Friday, July 23, 2004. See the Privacy International report on this issue at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-66860
[37] http://www.lifeandliberty.gov
[38] "Bush Calls for Extension of Anti-Terrorism Law; Kerry Criticizes Iraq Policies", Scott Stearns, Voice of America News, April 17 2004.
[39] "Patriot (Act) Games", Editorial, Washington Post, September 11, 2003.
[40] S.1709, 108th Congress 1st Session.
[41] 108th Congress 2nd Session.

powers of 'sneak and peak', roving wiretaps, and access to data held by businesses and libraries, Attorney General Alberto Gonzales argued that these changes would "make it more difficult to protect our country."[42]

Even as they recognise the value of the Patriot Act to protect the country, some members of industry have also weighed in to support the Senate initiative. In particular an industry coalition has called for changes to the Government's powers as they are concerned that

- Section 215 of the Patriot Act allows access to business records whenever the Government merely certifies that it is relevant to an authorized investigation, without having to provide underlying facts for the court or judge, with no limit on the breadth of records sought, whether privileged or proprietary;

- Section 505 allows federal agents to use 'National Security Letters' to obtain business records, including credit reports, customer records of communication service providers, and records of financial institutions without court approval and without a meaningful right to challenge.[43]

Concern regarding these access powers is spread across the political spectrum. Civil liberties organisations have placed pressure on Congress, appealed to the courts on grounds that the powers are unconstitutional; libraries have protested by putting up signs notifying customers of the possibility of surveillance; the media has highlighted potential abuse; and members of Congress have demanded greater reporting from the Department of Justice; amongst many actions by a variety of interested parties. These two powers will be reviewed in below.

Access to library records

Access to records held by third parties is perhaps the most controversial application of the Patriot Act. The controversy has focused mostly on whether the Department of Justice and the FBI may gain access to library borrowing records and data of internet transactions, i.e. email logs and website visits. The emphasis on libraries is curious but proponents of the power believe that their case is strong. One such proponent, Senator Kyl, went so far as to introduce a bill to preserve this power as other bills in Congress were threatening it.

> "[W]e should not forget that terrorists and spies historically have used

[42] "Gonzales Faults Senate Version of Patriot Act Legislation", Dan Eggen, Washington Post, August 30, 2005.
[43] Re: Sections 215 and 505 of the Patriot Act , a Letter to The Honorable Arlen Specter, Chairman of the Senate Judiciary Committee, from: Association of Corporate Counsel, Business Civil Liberties, Inc., The Financial Services Roundtable, National Association of Manufacturers, National Association of REALTORS, United States Chamber of Commerce, October 5, 2005.

> libraries to plan and carry out activities that threaten U.S. national security. We know, for example, that some terrorists have used computers at public libraries to use the internet and communicate by email. It would be unwise to place libraries and bookstores beyond the scope of anti-terror investigations."[44]

Section 215 of the Patriot Act permits the Federal Bureau of Investigations (FBI) to gain access to any relevant tangible item held by a business. This data can be accessed after a special judge reviews the request (though it is well known that such judges have almost never refused search request), and that the request applies to foreigners and the investigation relates to foreign affairs or national security, or that it applies to U.S. citizens but the investigation is related to international terrorism. The Patriot Act does have a disclaimer however: the investigation must not be based solely on the American's exercise of his or her free speech rights.

The gag order is a key component of the law. Those who are receiving the request to hand over the data are prevented from disclosing the existence of the order. This prevents the individual who is the subject of the investigation from questioning the grounds for which the data is to be disclosed: he is never notified of the search in the first place.

It is argued that the Patriot Act did not in fact revolutionise the law.[45] The power for such secret searches reviewed by a secret court has existed since the 1970s.[46] Law enforcement agencies' ability to access communications data (e.g. logs of communications and interactions) was first introduced in the 1980s.[47]

One innovation, and the rise of the controversy is that this data could be requested from libraries and other institutions where free expression rights are affected. Another innovation is the advance of technology: some feared that law enforcement agents could have access to increasingly sensitive information under too weak a privacy protection regime.

The American Library Association lobbied intensively to change the Act. Some librarians printed thousands of bookmarks with information on the Act, and others put up signs notifying patrons of their concerns. Others bought shredders to destroy logs of people who signed up to use the internet in libraries.[48] Eventually the 64,000 members of the American

---

[44] Statements on Introduced Bills and Joint Resolutions, S. 2476. A bill to amend the USA PATRIOT Act to repeal the sunsets; to the Committee on the Judiciary, Congressional Record, May 21, 2004, page s6096-S6099.

[45] For an excellent exposition of this perspective see Orin S. Kerr's "Internet Surveillance law After the USA PATRIOT Act: The Big Brother That Isn't", Northwestern University Law Review, Vol. 97, No.2, 2003, page 607-676.

[46] Coming from the Foreign Intelligence Security Act 1978.

[47] In the Electronic Communications Privacy Act of 1986.

[48] Librarians Use Shredder to Show Opposition to New FBI Powers", Dean E. Murphy, The New York Times, April 7, 2003.

Library Association formally denounced section 215 and lobbied Congress for its repeal. They were also joined by the American Booksellers Association.[49]

The Bush Administration rejected all these criticisms. First they argued that powers to request information from businesses have long existed in U.S. law, even under environmental regulations. All the Patriot Act permitted, the Administration claimed, was that this power was to be extended to combating terrorism.

Second the Bush Administration repeatedly noted that the power has seldom been used. In 2003, then-Attorney General John Ashcroft responded to the concern that libraries were under siege from requests.

> "The fact is, with just 11,000 FBI agents and over a billion visitors to America's libraries each year, the Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans.
>
> No offense to the American Library Association, but we just don't care.
>
> The charges of the hysterics are revealed for what they are: castles in the air built on misrepresentation; supported by unfounded fear; held aloft by hysteria."[50]

His speech on the matter followed the release of a memo showing that the power had never been used at all. He was thus able to argue that the librarians were caught up in "baseless hysteria".[51]

What is surprising to many is that the Administration had previously rejected calls for disclosures on the use of the Patriot Act powers. Yet even supporters of the Bush Administration in the House of Representatives repeatedly demanded some reporting on the amount of times these powers were used. The Chairman of the House Judiciary Committee, James Sensenbrenner Jr., a leading Republican, noted that "[t]he burden is on the Justice Department to show they are using their authorities in a lawful, constitutional and prudent manner."[52]

The Justice Department reported again on the usage of the powers in time to inform the debate on sunset provisions and to dissuade Congress from passing new bills threatening the Patriot Act. As of March 30 2005, the power to gain access to records under Section 215 had been used on 35 occasions but had not yet been used to gain access to

[49] "Librarians Make Some Noise Over Patriot Act", Rene Sanchez, Washington Post, April 10, 2003.
[50] Patriot Monitoring Claims Dismissed: Government Has Not Tracked Bookstore or Library Activity, Ashcroft Says, Dan Eggen, the Washington Post, September 19, 2003; Page A02
[51] "Patriot Act, Part II, Editorial, New York Times, September 22, 2003.
[52] "Fierce Fight Over Secrecy, Scope of Law", Amy Goldstein, Washington Post, September 8, 2003.

information regarding library borrowing privileges, bookstore sales, guns sales, or medical records.[53]

Self-certifying Access: National Security Letters

The Bush Administration's response to concerns over Section 215 of the Patriot Act are precise, though inaccurate. The University of Illinois did a survey of 1,020 public libraries and found that in the months after September 11th 85 libraries had been asked for information about patrons, relating to the attacks.[54] In June 2005 the American Library Association released a survey of 1500 public libraries and 4000 academic libraries and found that law enforcement officials had made over 200 formal and informal inquiries. Details on these inquiries were not released for fear that the librarians would be accused of criminal behaviour.[55] Reconciling these findings with the Government's statement of two months earlier on the use of Section 215 of the Patriot Act only requires looking at the alternatives.

Instead of using Section 215, the Department of Justice uses the 'National Security Letter' regime which has similar powers though even more limited oversight. NSLs are a form of administrative subpoena. They permit investigators to demand records without judicial approval but rather through a self-certification process, while prohibiting recipients of the letter from disclosing the request. There is no procedure by which to quash the demands and there is no exception to the gag order even for consulting an attorney.

The Justice Department have repeatedly declined to identify how many times NSLs have been used to seek or obtain information from libraries or other institutions.[56] The Government did release a document listing all the NSLs issued from October 2001 and January 2003 but the entire substance of the document was redacted, though the number listed was 'in the hundreds'.[57] There are now reports that more than 30,000 NSLs are issued per year.[58]

National security letters (NSLs) first became law in the 1978 Right to Financial Privacy Act. It was then applied to communications transactions in the Electronic Communications Act 1986, and are now part of the U.S. Code (18 USC section 2709). Both laws were created to protect privacy of transactions and thus regulated access to transaction data. In 1993

---

[53] "CRS Report for Congress: Libraries and the USA Patriot Act", Charles Doyle, Order Code RS21441, July 6, 2005.
[54] "FBI Begins Visiting Libraries", Christopher Newton, Associated Press, June 24, 2002.
[55] "Libraries Say Yes, Officials Do Quiz Them About Users", Eric Licthblau, The New York Times, June 20, 2005.
[56] "Library Challenges FBI Request", Dan Eggen, Washington Post, August 26, 2005."
[57] Page 63 of decision in *John Doe v. Ashcroft*, decided by U.S. District Judge Victor Marrero, 04 Civ. 2614.
[58] "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans", Barton Gellman, Washington Post, November 6, 2005, page A01.

the power was expanded slightly to allow the FBI to use NSLs to gain access to data on people who are in contact with terrorists or spies, not merely the spies and terrorists themselves.

Section 505 of the Patriot Act was the largest change to the law. The Patriot Act amended the NSL-regime by reducing the oversight while increasing the breadth of data that could be accessed.

- Communications data i.e. information about telephone calls, emails, internet transactions, etc., may be accessed, though this no longer requires authorisation from the Deputy Assistant Director of the FBI; rather an FBI field-bureau chief can authorise such a letter.

- Financial records and Consumer credit reports may now be accessed with authorisation by the Deputy Assistant Director or a Special Agent in Charge of a field office.

Generally the records sought must now only be 'relevant' to an authorized investigation to protect against international terrorism or foreign intelligence operations. Like section 215 it requires that the investigation of an American must not be solely upon the basis of activities involving free expression, though this restriction does not apply to non-Americans. A further policy change took place in 2003 when the Attorney General rescinded a previous practice that required the data to be destroyed and no longer disseminated when it was not relevant to the purposes for which it was collected. The new policy now permits the data to be retained by the FBI and disseminated freely among federal agencies.

NSLs are most controversial when applied to data held by internet service providers and libraries. Department of Justice investigators may seek to identify users and gain access to records of communication transactions, lists of books borrowed, and internet sites visited. According to the American Civil Liberties Union, access to this data could have a chilling effect on free expression. According to staff attorney Jameel Jaffer:

> "If the government monitors the Web sites that people visit and the books that they read, people will stop visiting disfavored Web sites and stop reading disfavored books. The FBI should not have unchecked authority to keep track of who visits [al-Jazeera's Web site] or who visits the Web site of the Federalist Society."[59]

Legal questions also focus on the fact that a gag order is in place against the recipient of the

[59] "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans", Barton Gellman, Washington Post, November 6, 2005, page A01.

NSL. This has led to a number of legal cases except that the plaintiff in the legal case can not be identified for fear of being in breach of the gag order. For instance, the ACLU is representing an anonymous plaintiff in *John Doe v Gonzales.*

In cases that are not related to terrorism, law enforcement agents would have to obtain a court order to gain access to transactional data by articulating "specific and articulable facts showing that there are reasonable grounds to believe that" the information sought is "relevant and material to an ongoing criminal investigation." A gag order is also possible, but again requires a court order and only in circumstances where the court deems it appropriate.[60] Active recording of communications data must also be sought through a court order but in this case the government need only show that the information is likely to be obtained by the collection of data and use is relevant to an ongoing criminal investigation."[61]

Though this route to demand data is not new, the significant difference between the general criminal and terrorism uses of administrative subpoenas is that unlike in their use under the Patriot Act, when an administrative subpoena is used in criminal cases a neutral tribunal determines, after the fact, whether its issuance is compliant with the constitution. The subpoenaed party must be able to obtain judicial review of the reasonableness of the demand.[62] In terrorism investigations NSLs are issued by the FBI and there is no judicial review. Recipients of NSLs do not have the ability to challenge the request. And the subjects of NSLs are never notified of the surveillance so will never be in a position to protest.

Non-governmental organisations and industry representatives have co-operated extensively in calling this practice into question. They have brought these issues to the media and even before the courts to question whether NSLs are constitutional. Appealing to the right to free speech and the right of anonymity that has been preserved by the U.S. Supreme Court's jurisprudence[63] these organisations argue that an un-regulated means of accessing personal information is unconstitutional. Their contention is that if data is to be accessed regarding the free expression activities of individuals then the constitution requires heightened evidentiary showing from the party seeking the subpoena before their

[60] Page 33 of decision in *John Doe v. Ashcroft*, decided by U.S. District Judge Victor Marrero, 04 Civ. 2614.
[61] ibid, page 34.
[62] ibid, p.50
[63] For an overview of the jurisprudence, see "Politics of the Information Society", Gus Hosein, a report commissioned by UNESCO, February 2004, available at http://unesdoc.unesco.org/images/0013/001375/137516e.pdf.

enforcement to identify anonymous speakers.[64] They argue that this is particularly necessary for the Internet where data about an individual's activities whilst on-line are even more sensitive.[65]

In November 2004 the District Court for Southern District of New York agreed with the NGOs in the case of *John Doe v. Ashcroft*.[66] The case involved a demand by the FBI upon an internet service provider who could not be named but who was represented by the American Civil Liberties Union. The plaintiff received an NSL demanding "any and all subscriber information, billing information, and access logs of any person or entity" associated with a specified internet IP address.

The Court found that NSLs lacked effective process and thus violated the constitutional protection against unreasonable search and seizures. The Court also found that subscribers' rights to free expression were threatened.

> "For example, the FBI theoretically could issue to a political campaign's computer systems operator a §2709 NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL under §2709 to discern the identity of someone whose anonymous online web log, or "blog," is critical of the Government. Such inquiries might be beyond the permissible scope of the FBI's power under §2709 because the targeted information might not be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, or because the inquiry might be conducted solely on the basis of activities protected by the First Amendment. These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight."[67]

The court expressed concern that some disclosures may reveal information protected by the subscriber's attorney-client privilege, e.g. the subject line of messages could convey privileged and possibly incriminating information. The Court concludes:

> "Considering, as is undisputed here, the importance of the internet as a forum for speech and association, the Court rejects the invitation to permit the rights of internet anonymity and association to be placed at such grave risk."[68]

---

[64] Brief of the Electronic Frontier Foundation, et al., In support of Appellees and Affirmation of Judgment Below, in case of Gonzales v. John Doe, United States Court of Appeals for the Second Circuit, 05-0570-cv, August 3, 2005.
[65] C.f. Alberto Escudero-Pascual and Ian Hosein, "The hazards of technology-neutral policy: questioning lawful access to traffic data", The Communications of the ACM, vol.47 no 3, 77-82.
[66] Decided by U.S. District judge Victor Marrero, 04 Civ. 2614.
[67] Page 75 of decision in *John Doe v. Ashcroft*, decided by U.S. District Judge Victor Marrero, 04 Civ. 2614.
[68] Page 78 of decision in *John Doe v. Ashcroft*, decided by U.S. District Judge Victor Marrero, 04 Civ. 2614.

The Court thus enjoined the Justice Department from issuing NSLs. On appeal the Court stayed the ruling.

The case was then taken to the U.S. Circuit Court of Appeals. The ACLU and Doe, by this time joined by the American Library Association, made an emergency appeal to the Supreme Court to be freed from a gag order in order to participate in a congressional debate over the Patriot Act particularly as its sunset approaches. On October 7 2005 the Supreme Court denied the emergency application to vacate a stay in the challenge. In an unprecedented motion, the Supreme Court stated its case for denying Doe from identifying himself: nothing prevents the American Library Association from lobbying Congress by stating that one of its members has been served with an NSL, it is not essential that Doe be identified while the case is still being decided in the Courts.[69] The case was returned to the Circuit Court at the time of this report's release.

In the meantime another set of court decisions were handed down that further restricted the Government's ability to gain access to communications data. In two separate court decisions, the courts upheld the right of the FBI to gain access to traffic data under the weaker tests of the Patriot Act, but the courts both held that some data was more sensitive than others and thus deserved greater protections and safeguards provided under the Constitution. Location data generated by mobile telephony, the courts argued, can only be accessed under probable cause that a crime is being committed,[70] a far higher standard of proof.

The U.S. in Summary

This brief of the U.S. anti-terror policy landscape has left out much. We did not cover many of the proposed powers, existing powers, and legal cases. We did cover sufficient examples to draw some conclusions.

Though to the rest of the world the U.S. is leading by example through the establishment and use of extensive powers of surveillance, the reality is that situation in the U.S. is quite erratic with a number of proposals set out and some face a public demise whilst some that are even worse do not receive any public scrutiny. Attention to CAPPS II was intense yet

[69] Supreme Court of the United States, Justice Ginsburg deciding as opinion in chambers, *John Doe v. Gonzales*, on Application to Vacate Stay, No.05A295, 546 U.S. 2005.

[70] United States District Court Eastern District Of New York, In The Matter Of An Application Memorandum Of The United States For An Order And Order (1) Authorizing The Use Of A Pen Register And A Trap And Trace Device And (2) Authorizing Release Of Subscriber Information And/Or Cell Site Information, Decided by James Orenstein, Magistrate Judge, M 05-1093 (JO), October 24, 2005; and United States District Court Southern District of Texas Houston Division, In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, Magistrate No. H-05-557M, October 14, 2005.

there was little discussion of US-VISIT. Similarly, the USA-PATRIOT Act was much debated and discussed yet the Enhanced Border Security and Visa Reform Act was not. There is a rich debate in the U.S., though sometimes it is poorly focused.

Within the fray of policy debate in the U.S., one conclusion that can be drawn is that the more a policy is debated the greater the likelihood of criticism and change. This is supported by a study from the University of Connecticut's Center for Survey Research & Analysis found that the more the public knows about the Patriot Act the less they support it. In particular, the researchers found 'substantial opposition' to the components of the law discussed in this report. While over 70% supported the law, when told in detail what it constituted, 52% supported access to library records without notification to the patrons, 43% supported access to data under NSLs, and 23% supported secret searches. In fact only 14% supported the Patriot Act as a whole once they were informed of its components. Half of those surveyed believed that Muslim and Arab Americans would be targeted, while 40% believed that Iraq war protesters will be investigative targets too. Only 13% felt that 'ordinary Americans' would be targeted.[71]

In the U.S. we also see substantial forms of political and legislative activity. Non-governmental organisations are drawing coalitions with others of different political stripes, and are also aligning with industry and policy experts to question policies. Cases are being brought before the courts. Media attention is at times intense. Lobbying occurs and Congressional action follows where bills are introduced to minimise harms to civil liberties and to clarify powers established in more uncertain times.

This is not to say that everything is getting better. Means are still used to minimise debate. REAL ID was passed only because it was appended to a bill for funding the war in Iraq and Tsunami relief. The U.S. implemented biometric passports on RFID chips despite over 90% of consultation responses opposing this development on privacy grounds.

But the general conclusion is that there is a great debate occurring in the U.S. regarding anti-terrorism powers and in particular their effects upon free expression and freedom of movement. An aware and active populace is a significant check and balance on the actions of a Government, even at times of war.

[71] "University of Connecticut Releases New National Poll on the USA PATRIOT Act", University of Connecticut Center for Survey Research and Analysis, Samuel Best and Monika McDermott, August 26, 2005.

What Europe is Doing

The policies introduced in Europe are in many ways similar to many of the policies proposed in the U.S., though the legal and political landscapes are remarkably different. Each legislature in each European Union Member State has introduced legislation to respond to terrorist attacks in 2001 but also to subsequent attacks across Europe.

The list of changes in each country is long; here we mention merely a few. The French introduced blanket communications surveillance, and the power to expel extremists, and is now proposing to increase video surveillance in public areas, and to monitor suspects' travel.[72] Germany's opposition party proposed a power of two-year preventive arrest,[73] while the German government has been banning anti-semitic organisations.[74] Greece rushed to approve new anti-terror rules before the 2004 Olympics due to pressure from the EU to implement measures for a pan-European arrest warrant, extradite Greek nationals, freeze of accounts, and introduce biometric passports.[75] Italy has conducted immigration crackdowns, required ID cards in cyber cafés, instituted deportation powers, and called for more CCTV surveillance. In the Netherlands identity requirements were introduced, the Government proposed to regulate the movement of suspects and require regular reporting to the police,[76] and considered a blasphemy law.[77] Spain outlawed some political parties, and proposed to register all clergy members, places of worship and monitor all sermons.[78]

While Member States have been busy, a significant source of policy is the European Union itself. The European Union's processes for the establishment of policy and legislation is at a critical phase and is continually dogged by claims of a lack of democratic accountability. There are currently three separate powers in the EU. Under the current system, the Council of the European Union ('the Council') consists of the ministers and government representatives of the Member States. It has a rotating Presidency, each for six-month periods, currently resting with the UK and to be followed by Austria. The European Commission also proposes and implements legislation, and is independent of Member States by design. Finally, the European Parliament sometimes approves and is consulted on legislation, though it can not initiate legislation.

---

[72] "France Considers Anti-Terrorism Measures", Lisa Bryant, Voice of America, October 26, 2005.
[73] "CDU Wants 2 Yrs Preventative Arrest, Polemics Ensue", AGI, May 25, 2004.
[74] "Germany Imposes Ban on Islamic Group", Geir Moulson, AP, January 15, 2003.
[75] "EU blast draws pledge for stricter law on terrorism", Kathimerini English Edition, June 9, 2004.
[76] "Out to thwart terrorism - the Dutch cabinet's new plans", Hans de Vreij, Radio Nederland, January 26, 2005.
[77] "Blasphemy law revival upsets the Dutch elite", Ambrose Evans-Pritchard, Daily Telegraph, November 18, 2004.
[78] "Spain Weighs Muslim Rights and Concerns About Safety", Dale Fuchs, The New York Times, May 23, 2004.

The EU has created a great deal of legislation that Member States must then transpose into national law. For instance, in June 2002 the Framework Decision on combating terrorism came into force, compelling all Member States to comply by December 31, 2002. The Framework Decision offers a definition of terrorist offences, terrorist groups, offences relating to terrorist activities, and penalties.[79] At the same time the European Parliament also approved a European Arrest warrant framework decision with little debate. Both these documents raised concerns amongst civil liberties organisations on how they would affect the right to protest but little debate occurred on either policy.[80]

There is a conflict of laws between many of the surveillance policies emerging from the EU and the existing privacy protection regimes. Building on the right to privacy contained in the European Convention on Human Rights[81] the EU established a Directive on privacy and data protection in 1995. Both these regimes are supposed to limit the breadth and scope of surveillance.

The reality is that the existing privacy regimes have not limited the breadth and scope of the policies placed before the legislative bodies at the EU. Some policies are remarkably similar to those in the U.S. while some go even further. A significant proportion of the current policy activity is now taking place under the Hague Programme.

Setting the Landscape: The Hague Programme

In November 2004 the European Council announced the Hague Programme for *Freedom, Justice and Security*. This programme is the EU's strategy for enhancing security over a five-year period, by enhancing co-operation in justice and home affairs. It was created behind closed doors and was released to the public only right before it was approved by the Council. While the preceding programme, the Tampere Programme from 1999 had as its core value the respect for the rule of law, this was removed in the Hague Programme in favour of an emphasis on 'cross border problems' such as illegal migration, terrorism and organised crime.[82] The programme's stated objectives thus include the regulation of migration flows, control of the external borders of the Union, the fight against organised cross-border crime, repression of the threat of terrorism, realisation of the potential of cross-border police agencies, the increase of co-operation in criminal and civil matters.

With the intention of turning the programme's broad principles into 'concrete action', in

[79] Council Framework Decision of 13 June 2002 on combating terrorism, 2002/475/JHA, Official Journal of the European Communities, L164/3.
[80] "EU definition of "terrorism" could still embrace protests", Statewatch, December 13, 2001.
[81] A Council of Europe convention that all EU Member States have ratified.
[82] "A response to the Hague Programme: Protecting the Rule of Law and Fundamental Rights in the Next Five Years of an EU Area of Freedom, Security and Justice?", Liberty & Security, November 2004.

May 2005 the European Commission launched its 5 year Action Plan for Freedom, Justice and Security. It contained detailed proposals for EU action on terrorism, migration management, visa policies, asylum, privacy and security, the fight against organised crime, and criminal justice.

Some of the more problematic powers include the increase of international data sharing while lacking adequate controls such as dual criminality and adherence to national law, and increased monitoring of communications and financial transactions. Though not all the initiatives at the EU fall within the Hague Programme, the programme will play a decisive force in the future. The larger spectrum of activities on anti-terror policy is addressed below.

Monitoring Travel and Movement

Like the U.S., the EU is actively enhancing surveillance of travel and at borders. While it initially responded with alarm to the requests from the U.S. for passenger data it turned about and began considering access to the same data. Similarly, the EU is beginning to collect biometrics as well.

Logging of Movement: Passenger Records

The U.S. law on transportation security included a demand for access to passenger name records (PNR) from foreign carriers. This data would be used to analyse the names and details of all arrivals and departures from the U.S. At first the EU opposed the transfer of this data from EU carriers' reservation databases to the U.S. Department of Homeland Security on grounds that the transfers would be in breach of EU privacy protections that prevented the further processing of this data without adequate safeguards. This led to intense negotiations between the European Commission and the Department of Homeland Security.

As time went on, the European Commission grew concerned that it could not continue its opposition to the U.S. plans for access to passenger data. Apart from the threatened sanctions, it emerged during the negotiations that the European Commission wished to create a policy similar to the U.S. policy it was opposing. In fact, the Commission grew reluctant to refuse to the U.S. government access to the data on these very grounds. When negotiating with the U.S. to limit access to 'sensitive information' such as religious faith (as ascertained by the dietary choice, e.g. Halal or Kosher), the head of the EU's Directorate General for Internal Market, Commissioner Bolkestein informed the European Parliament that the EU must be careful in what it refused to the U.S.:

> "The EU cannot refuse to its ally in the fight against terrorism an

> arrangement that Member States would be free to make themselves."[83]

Pressure was rising from EU Member States, and from other sections of the European Commission. The final Communication from the Commission later stated that the agreement

> "with the US appears to be a sound basis for taking forward work on an EU approach (...). The list of data elements also seems broad enough to accommodate law enforcement needs in the EU. Nothing in the arrangements agreed with the US therefore seems to prejudice the development of an appropriate EU policy."[84]

In fact the Commission began calling for a resolution to the U.S. transfer problem by creating a centralised system where all PNR for all EU carriers could be sent first to a central database and then sent onwards to the U.S. Not only would this be beneficial in terms of cost and efficiency, then Vice President of the Commission Loyola DePalacio claimed that the centralised approach would save money for airlines and the EU as it would also assist in "adopting a community policy in the field of data processing with a view to control immigration".[85]

The Justice and Home Affairs Commissioner went a step further.

> "As a matter of fact, I can even see that a centralized structure inside European Union will be able to provide the necessary guarantees on the liability aspects, the accuracy of the data on the security of transmitted data, the technological means and the filters that Vice-President De Palacio has just mentioned to you, on the supervision by adequate control mechanisms, above all the role of the giant supervisory board and for offering added value to similar initiatives conducted at national levels within the European Union."[86]

The agreement with the U.S. was thus seen as a precursor to a European policy on access to PNR.

The EU policy, however, would not be restricted to combating serious crimes and terrorism, but could be used for any law enforcement purpose, including immigration. In September 2005 the UK Presidency of the Council proposed further use of PNR as a response to the

---

[83] F. Bolkestein, "Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market", Brussels: European Parliament, December 1, 2003.
[84] F. Bolkestein, "EU/US talks on transfers of airline passengers' personal data: Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market", Strasbourg: European Parliament, December 16, 2003.
[85] "Transcription of the committee meeting: European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market", Strasbourg: European Parliament, December 16, 2003.
[86] Ibid.

London-terror attacks, leading to an 'intelligence-led approach to border control'.[87] As a result the UK Presidency of the EU proposed the long-term retention of this data by border security agencies.

Registration of Movement

A key mission of the EU is to ensure the free flow of people across borders. The EU thus plays a role in the assurances and procedures established to manage border traffic. A significant portion of this activity began with the Schengen Agreement in 1985, and has since then continued with the establishment of new practices and systems.

The Schengen Information System (SIS) went live in 1995 and was seen as a compensation mechanisms for the removal of internal borders between France, Germany, Luxembourg, and the Netherlands. It permits Member States to obtain information regarding certain categories of persons and property. Member States contribute by adding data on people wanted for arrest, people to be placed under surveillance or subject to specific checks; people to be refused entry at external borders; and lost or stolen items. By 2003 it had files on 877,655 people, a further 386,403 aliases.[88]

Access to data on the SIS is limited to border authorities and police and customs checks. According to reports, EU officials acknowledged in 2003 that there are 125,000 access terminals.[89] Since then access has been extended to security and intelligence services. Europol, the European Law Enforcement Organisation,[90] had expressed an interest to gain access to the database to perform analysis involving relationships between relevant variables, comparing ethnic and demographic trends, and for statistical data. This form of access was denied.

As the EU grew a newer system was proposed: SIS II. Additional changes were introduced at this stage to allow for the storage, transfer and querying of biometric data such as photographs and fingerprints. SIS II is set to go live by 2006.

Registration of Foreigners

In response to the terrorist attacks in the U.S. in 2001, the EU decided to implement a Visa Information System (VIS). VIS would hold personal information on every visa applicant to an

[87] "Liberty and Security: Striking the Right Balance", A Paper by the UK Presidency, September 7, 2005.
[88] "Statewatch Analysis: From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained", Ben Hayes, February 2004.
[89] ibid.
[90] According to its website, Europol "aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organised crime." www.europol.eu.int.

EU member state including their nationality at birth, grounds for refusal, and links to other applications. It will be a central database that is complemented by national systems that together link border checkpoints of each country. It is designed to manage biometric data, i.e. photographs and fingerprints. By 2007 it will be processing 20 million visa applications annually, which would result in 70 million fingerprints to be stored for five-years periods.[91]

The Article 29 Working Party, a committee of privacy regulators from all the EU member states have raised a number of concerns regarding the proposed measures within VIS, in particular the collection of fingerprint data. The Working Party is concerned that the fingerprints could be used for other purposes, and could also lead to stolen identities. As such the Working Party recommends that biometric data should not be stored in the central database unless absolutely necessary. Rather the Working Party recommends that the biometrics be kept only on a microchip on the visa itself. The Working party was particularly concerned with the centralisation of biometrics because the access to the VIS was ad-hoc and wide.

Since the London bombings in July 2005 the momentum has grown for additional databases and tracking mechanisms. The UK Presidency of the EU has been calling for a broadening of the access privileges to VIS, permitting law enforcement agencies across the EU to access all data held there. The Presidency is also calling for similar access to the SIS II.

The UK Presidency of the EU is also calling for an entry-and-exit registration programme to keep track of those who have entered but not yet left. The use of biometrics is under consideration within a feasibility study due in December 2006.[92]

Meanwhile the United Kingdom is proposing an E-Borders programme that will integrate travel records with biometric scans. Her Majesty's Government already has access to passenger data for customs and immigration purposes and to combat terrorism; but now the Government is seeking to regularise the use of this data, compel the collection of biometrics of all visitors, residents, and citizens, and to use this data to, according to the Government, "support general police and criminal justice functions."[93]

Registration of Citizens: Passport and ID

The collection of biometrics in the EU is not being limited to visa-applicants and other

[91] Article 29 Working Party, "Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final), 1022/05/EN WP 110, June 23, 2005.
[92] "New ideas' on Counter-Terrorism from the July JHA Council: Next Steps", A note from the Presidency to COREPER, Council of the European Union, 1191/05, Brussels, September 2, 2005.
[93] The UK Home Office, Partial Regulatory Impact Assessment Data Capture And Sharing Powers For The Border Agencies, May 2005.

foreigners however. In its interpretation of the ICAO standard on secure passports the European Council decided in 2003 to develop a shared approach on biometric identifiers for documents for third country nationals, European Union citizens' passports and EU information systems (VIS and SIS II). In February 2004 the European Commission stated its intention to follow through by requiring all EU travel documents to include the biometric of a facial image, and thus to follow the Americans. Member States were permitted to go further by implementing fingerprints as well.

Months later the Council forced a change in strategy and ordered that both face and fingerprints be made mandatory for passports. The European Parliament opposed the inclusion of fingerprints and rejected the creation of a central database of EU passports and travel documents. The Council ignored their opposition and called for facial images to be included within 18 months and fingerprints within 36 months. In February 2005 the European Commission announced the schedule and details for the Council's plan.

So far, EU documentation points to the inclusion of only two fingerprints on a chip on the passport protected with a security mechanism called 'Extended Access Control'. This means that the data on the chip relating to fingerprint images can only be read by authorised entities.[94] The specifications of these security mechanisms remain unclear and are not discussed openly.

Meanwhile the UK Presidency, which began in June 2005 has promised to standardise identity card systems across the EU so that they also include fingerprints. The UK Presidency argues:

> "To turn our backs on proven biometric technology, to ignore the use made of fingerprints, iris and digital photos by both government and the private sector would be to reject the twenty-first century."[95]

The UK Presidency also calls for the verification of identity against a centralised database, even as the UK Parliament continues to debate whether or not to approve the implementation of biometric ID cards in Britain.

Data Mining and Profiling

In the debate over access to SIS and SIS II, there was some consideration of giving Europol vast access to the databases so that statistical analysis could be done through trawling the data. Though this was rejected on SIS, it is still being considered under SIS II.

---

[94] "EU-Passport Specification", Working Document, available at http://www.statewatch.org/news/2005/mar/biometric-implement.pdf

[95] "Liberty and Security: Striking the Right Balance", A Paper by the UK Presidency, September 7, 2005.

Despite its strong data protection and privacy legal regime, the European Union has also been considering computer-assisted profiling. Its purpose:

> "is to facilitate targeted searches for would-be terrorists (...). It is closely connected to the German initiative on computer-aided preventive searches carried out by individual Member States on the basis of coordinated offender profiles (Europe-wide electronic profile searches). Such searches are essential to the success of security service operations. (...)
>
> "On the basis of this profile each Member State searches the relevant national data bases (e.g. registers of residents, registers of foreigners, universities etc.) subject to the provisions of national law, for persons who need to be vetted more closely by the security authorities. The more detailed the offender profile, the smaller the group of persons covered by the search."[96]

The policy calls for increased data-sharing between EU member states and with Europol. In cooperation with Europol, the police would identify specific areas where the development of targeted terrorist profiles may assist the identification of terrorists.

> "Developing terrorist profiles means 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. It may therefore be necessary to develop the profiles in such a way that individual profiles cover a well-defined and specialised category of persons who fulfil a particular function within a closely defined area of terrorism. It will also be necessary to update the profiles as often as necessary so that they always give a correct picture of the particular characteristics of the category of persons in question."[97]

The EU identifies a number of 'elements' for these terrorist profiles, including nationality, travel document, method and means of travel, age, sex, physical distinguishing features (e.g. battle scars), education, choice of cover identity, use of techniques to prevent discovery or counter questioning, places of stay, methods of communication, place of birth psycho-sociological features, family situation, expertise in advanced technologies, skills at using non-conventional weapons, attendance at training courses in paramilitary, flying and other specialist techniques.[98] They would then search through national databases hoping to identify equivalent elements in order to then presumably pinpoint terrorists.

---

[96] Council of the European Union, Memo from German Delegation to the Article 36 Committee, Subject: Note on computer-aided preventive searches carried out by individual Member States on the basis of coordinated offender profiles (Europe-wide electronic profile searches), Brussels, October 31, 2002, 13626/02, LIMITE ENFOPOL 130.

[97] Council of the European Union, Draft Council Recommendation on the development of terrorist profiles, Brussels, 14 October 2002 11858/1/02, REV 1 LIMITE ENFOPOL 117.

[98] Council of the European Union, Draft Council Recommendation on the development of terrorist profiles, Brussels, 14 October 2002 11858/1/02.

This policy generated concern from the EU Network of Independent Experts in Fundamental Rights (CFR-CDF). In its first report from May 2003, the network argued:

> "The development of terrorist profiles on basis the characteristics such as nationality, age education, birthplace, psycho-sociological characteristics, or family situation - all these elements appear in the recommendation on developing terrorist profiles - in order to identify terrorists before the execution of terrorist acts and cooperation with the immigration services and the police to prevent or reveal the presence of terrorists on the territory of Member States, presents a major risk of discrimination. The development of these profiles for operational purposes can only be accepted in the presence of a fair, statistically significant demonstration of the relations between these characteristics and the risk of terrorism, a demonstration that has not been made at this time."[99]

In July 2003, the UK Government announced its participation in a pilot group comprising experts from a number of EU Member States to get this project off the ground.[100] Little has been reported on this matter since 2004.

Surveillance of Transactions

European institutions have long recognised the value of communications data and its relationship with free expression and the right to a private life. The committee of all the privacy regulators from the EU member states once stated that traffic data was deserving of special attention.

> "A feature of telecommunications networks and of the Internet in particular is their potential to generate a huge quantity of transactional data (the data generated in order to ensure the correct connections). The possibilities for interactive use of the networks (a defining characteristic of many Internet services) increases the amount of transactional data yet further. When consulting an on-line newspaper, the user 'interacts' by choosing the pages he wishes to read. These choices create a 'click stream' of transactional data. By contrast more traditional news and information services are consumed much more passively (television for example), with interactivity being limited to the off-line world of newspaper shops and libraries. Although transactional data may in some jurisdictions receive a degree of protection under rules protecting the confidentiality of correspondence, the massive growth in the amount of such data is nevertheless a cause of legitimate concern."[101]

Contrary to the jurisprudence in the U.S., traffic data is protected under the jurisprudence on human rights law from the European Court of Human Rights. Previously the Court

[99] "EU network of independent experts in fundamental rights" (CFR-CDF), First Report, May 2003.
[100] Written Question P-3694/03 by Sarah LUDFORD (ELDR) to the Council, Subject: Terrorist profiling, March 30, 2004.
[101] Article 29 Working Party, "Recommendation 3/97: Anonymity on the Internet," (Brussels: European Commission, 1997).

acknowledged in *Klass v. Germany* that because a law permitting interception of mail created a "menace of surveillance" for all users of the postal service, and because that menace struck at freedom of communication, the law therefore constituted an interference with the right to respect for private life. The *Klass* court also believed that traffic data was sensitive, and this was verified in *Amann v. Switzerland* when the Court ruled it was illegal for State security services to keep a record indicating that the applicant was a contact of the Soviet Embassy, after intercepting a telephone call from the Embassy to the applicant. The *Amann* court specifically noted that storage of the information on an index card alone was sufficient to constitute an interference in private life and that the subsequent use of the stored information had no bearing on that finding.

While the ECHR acknowledges that traffic data deserves protection, unlike in the U.S., the inverse actually happens in practice. After the Courts failed to protect the privacy of traffic data, the U.S., Congress developed a statutory right to privacy to prevent traffic data from arbitrary access and proposed that traffic data is collected when authorised by a court when the data is relevant to a specific investigation. The Patriot Act extended this (albeit weak) protection to modern communications systems. Meanwhile European governments are insisting on implementing mass surveillance of communications traffic data with as little oversight as possible.

Retention of Communications Traffic Data

Perhaps the most controversial policy being proposed in Europe is the retention of communications traffic data. One of the earliest forms of this proposal came from the UK Government in 2000, proposing that all communications service providers, i.e. telephone companies, mobile companies, internet service providers, and internet hosting providers, retain traffic data generated by their systems for period of 7 years so as to ensure that the data is available for law enforcement agencies. The Government worried that the data may be deleted because of privacy rules and business practices. This specific policy proposal never moved forward after outcries from civil liberties organisations and industry representatives.

After September 11 a number of European Member States moved to implement the policy of traffic data retention into national law. Some now have such regimes in place though the regimes are fragmented in their coverage: some only include mobile phone and landline communications data, others are comprehensive and include internet data. Some require retention periods of a few months, others for four years. Since 2003 the Council of the European Union has been working towards a harmonising measure to ensure that all Member States have a retention policy. By the time the UK Presidency began in June 2005, the Council was wavering between 1 and 4 years for retention, with disagreements on the

types of data to be retained, and possibly compelling the collection of data that communications providers did not actually collect. Regimes regulating access to the data was left to national law however. The European Parliament rejected the Council's retention proposal.

After the London bombings in July the UK Presidency of the EU convened emergency meetings on combating terrorism. Data retention was on the top of the agendas.[102] When presenting the path forward for the UK's Presidency of the EU, it called for Parliament to approve retention, identity documents, use of passenger data, and increased use of CCTV cameras.[103]

In September 2005 the European Commission entered the fray and declared that the Council had no role to play in data retention and instead announced its own policy on retention. The Commission's proposed Directive originally limited the retention period for mobile and telephone calls to one year and internet data for six months. Access to this data was to be restricted to terrorism and serious criminal investigations. In October 2005 the Council declared that it would call on the Parliament to approve the Commission Directive provided that the Commission Directive would meet some basic standards set out by the Council. This included a retention period of up to 2 years, while permitting even greater periods if passed by national law. If the Parliament failed to approve the measure in time, the Council announced it would reintroduce its own proposal. According to the Danish Justice Minister:

> "Are we most afraid of the European Parliament or of terrorism? We must reach a decision in December. If the European Parliament cannot help, then MEPs are not adult enough to take part in the discussion."[104]

At the time of writing this report, the final outcome on this political situation remained uncertain. Increased pressure was being placed on the Parliament to ensure that the proposals contained now safeguards in the form of authorisation requirements (e.g. judicial authorisation) and preventing any discussion of limiting the situations in which the powers can be applied (e.g. terrorism vs. general investigations).

While the Justice Ministers from Member States speak with such strong terms at the level of the EU, their actions at home do not reflect their words. Although some national parliaments have approved data retention, they are far from the majority. Even the United

[102] Press Release of the Extraordinary Council Meeting, Justice and Home Affairs, Council of the European Union, 11116/05 (Presse187), July 13, 2005.
[103] "Liberty and Security: Striking the Right Balance", A Paper by the UK Presidency, September 7, 2005.
[104] "Clarke threatens MEPs over EU terror laws", Jenny Booth, The Times, October 12, 2005.

Kingdom Parliament has not introduced a law that requires telecommunications service providers to retain traffic data; rather such a regime is merely voluntary and for a varying period of time (up to one year). Very few countries have a mandatory regime, and of those that do, they have yet to enforce the law, or to apply the policy to all telecommunications. For instance, Ireland has retention for three years, but only for telephone and mobile phone data, not for internet transactions. Ministers are pushing the European Union to adopt a policy that their own Parliaments have failed to approve.

It is certain that if the EU agrees on a policy on retention then all Member States will have to implement a national policy. For instance, the Irish Justice Minister admitted in his own Parliament that he was awaiting the 'EU cavalry' to come to his aid and when it had failed to do so because of a lack of agreement amongst Member States, he was compelled to introduce a law on retention under a late amendment to terrorism legislation.[105] Yet the Irish Government and the Minister is insisting that the European Parliament push through a retention policy with a greater ambit than Ireland's own law[106] claiming that otherwise the EU is infringing upon the sovereignty of Ireland.[107]

Access to Communications Transactions

Unlike in the U.S. very little of the debate in the EU on data retention and communications privacy has looked at free expression. The potential chilling effect on communications and access to information would be remarkable if individuals knew that their transactions would be kept for an extended period of time. Yet if it is merely retained for the purpose of national security and combating terrorism then many would deem this acceptable, much as section 215 of the Patriot Act requires relevance to a terrorism investigation and a judicial authorisation.

Apart from the fact that the U.S. has not instituted data retention, more importantly the U.S. restricts access to traffic data by requiring court orders; and only in terrorism investigations is this requirement watered down somewhat. In Europe traffic data will be used for all investigations and will not necessarily require judicial authorisation. In some European countries, for instance, traffic data is authorised by senior police officers, with greater ease and broader applications than the controversial NSLs in the U.S.

One of the greater differentiators between the Council and the Commission proposals on

[105] Mr. Michael McDowell: "There is no EU cavalry coming down the hill to help me. I must sort out this conflict." Stated in Seanad Debate, Volume 179 No.4, February 3, 2005.
[106] "Clarke threatens MEPs over e-mail and phone records law", David Rennie, Daily Telegraph, October 13, 2005.
[107] "EU justice ministers agree compromise on data retention", Teresa Kuchler, EUObserver.com, October 13, 2005.

data retention is that the Council plans leave regulations on access to be decided by national law. The Commission intended that the data would only be accessed for use in terrorism and serious criminal investigations. In this domain the European Commission has no jurisdiction, however, as it is up to the Governments of the Member States and their Council of the EU to decide on access due to the legal structure of the EU. This leads to a situation where the European Commission and the European Parliament may approve data retention for the purpose of terrorism even though the data will be accessed under countless circumstances because the Council has refused to limit the use of traffic data to combating terrorism. Put more simply: a law passed to combat terror will be used any way that the Government sees fit.

The UK Presidency of the EU is particularly attentive to this approach because the UK is a case in point. In the UK's Anti-Terrorism Crime and Security Act 2001, the UK's response to the September 11 attacks, Parliament approved voluntary data retention by communications service providers for the purpose of preserving national security and combating serious crime. But access to this data is instead regulated by the Regulation of Investigatory Powers Act 2000 which permits wide access to traffic data held by communications service providers. Prior to the RIP Act the police would expect voluntary compliance from communications service providers when they were asked for traffic data; the RIP Act made the disclosure of this data mandatory, even as it failed to require judicial authorisation. ACTSA vastly increased the amount of data stored in the first place.

When the public caught on to the fact that the law was passed to combat terror could be used to combat crime, a furore arose. The UK Government then opened a national consultation to review and revise this situation. The rules remained relatively unchanged. Under a statutory instrument established in 2003, now sixty-one different types of agencies and departments can access various types of retained transaction data.[108] Local councils, environmental agencies, and health inspectorates may access data without any form of judicial authorisation. It is highly unlikely that even after ignoring the national consultative process and opposition that the UK Government will entertain any additional safeguards and restraints on the access powers because of any changes in EU law.

On top of making the data accessible for all investigations, the EU is working on ensuring that data is shared between Member States' police forces under the 'principle of availability': this principle expands data-sharing by requiring that if data is accessible to the French police in France under French law then the French have the right to demand the British Police to seek the data from a British service provider, even if there is no similar power

[108] c.f. The Regulation of Investigatory Powers (Communications Data) Order 2003, Statutory Instrument 2003 No. 3172.

under British law. This will ensure that the weakest safeguards in the EU will apply across Europe.

Summarising Europe

European policy is increasingly taking place in closed institutions with little debate. Policies of significant concern for the freedom of movement and freedom of expression are being made with little consultation.

The Hague Programme is seen as having a momentum of its own: what was decided by the Council is marching onwards towards legislation. Parliament and other institutions are warned that they may not change the direction of the policies agreed and enshrined into the Hague Programme. Just as fingerprints were included into passports without the consent of Parliament, so it looks that communications traffic data will be retained without adequate scrutiny of Parliament.

Even when the EU is called upon to decide between conflicting laws, as it was in the case of access to passenger records, it chose to agree to the U.S. demands so as to permit the creation of a policy of access to that same data by Member States.

Finally when European governments approve a policy for use to combat terror, it rarely restricts it to counter-terrorism. Passenger data, profiling, biometrics collection and access to communications data all start with anti-terror laws but are routinely used for all lawful purposes.

What Europe suffers most greatly from is that the conduct of the European Union lacks public scrutiny. Media coverage of EU issues is limited; non-governmental organisations tend to be national in nature and lack access to EU institutions; and the European Parliament is rarely given the necessary amount of authority to decide on these policies. When it comes to anti-terrorism policy, the EU is a game for Member States governments not for public oversight.

Summary and Conclusions

Both the U.S. and the Europe have implemented far reaching powers in the name of combating terrorism. In many areas they have implemented similar policies. They have both used strategies to lessen debate, either through appending bills to spending measures (e.g. REAL ID Act in the U.S.) or approving a policy at a closed-door international forum despite the protestation of Parliaments (e.g. Passenger data, biometric passports, and communications traffic data retention at the EU). If there is one remarkable difference between the two it is that when the U.S. goes too far on a policy and controversy arises, eventually public discussion and the democratic process tends to restrain the powers of Government. There is no similar policy deliberation process in Europe.

The table below compares the various regimes and the policies implemented in the U.S. and Europe. It is fair to say that although the U.S. is often maligned for its anti-terror policies, the EU always goes much further.

Table 1 Variation of Powers

Policy	U.S. Implementation	EU Implementation
Access to communications (purpose and oversight)	Under a court order if requiring communications traffic data that is related to an investigation; location data appears to require probable cause; self-certification under law for terrorism and foreigners only using NSLs.	Access provided for location, internet, and call data for the purpose of any investigation. No requirement for judicial authorisation; self-certification for all investigations in some countries.
Retention of Communications Transaction Records	No policy. Data is retained for law enforcement purposes upon issuance of a court order for a 'pen register' to initiate collection.	All data on all users to be kept by service providers for up to four years.
Data Mining	TIA withdrawn funding, CAPPS II failed, MATRIX removed from service.	Still under active consideration while ensuring sharing of database access across borders and ensuring police have access to visa and immigration files on VIS.
Access to Passenger Data	For combating terrorism and serious organised crime.	For general policing purposes and immigration controls.
Biometric Registration at Borders	Registers biometric data and travel-related data on foreigners, with the exception of Canadians and Mexicans. Not applies to U.S. citizens.	Establishing an EU-wide system of registration for all visitors, residents and citizens involving passenger data and biometric data.
Biometric Identity Documents	Facial recognition involving digital photographs in U.S. passports and no central database for verification.	Facial recognition and fingerprints in all passports. Back-end database planned.

The above table shows that the situation in Europe appears to be worsening even as the U.S. tries to rectify some of its prior transgressions. It is possible to explain this through the variances in the political processes in each case, as described by the following table.

Table 2 - Quality of Debate on Policies

Policy	U.S. Policy Deliberation Dynamics	EU Policy Deliberation Dynamics
Access to communications (purpose and oversight)	Legislation proposing safeguards, years of congressional debate, high media awareness, local campaigns, court cases.	European Council is coercing European Parliament so as to avoid any discussion on this matter.
Retention of Communications Transaction Records	No policy.	European Council is calling on the European Parliament to agree to Council demands or else the Parliament will be removed from the process.
Data Mining	Intense media and NGO activity, Congressional scrutiny, governmental reports.	None.
Access to Passenger Data	Little debate on access to foreign carriers; larger debate on access to travel profiles and data stores of domestic travel with NGO activity, media attention and court cases.	Much debate on U.S. access to information on Europeans, but no debate on equivalent access by EU.
Biometric Registration at Borders	Little debate.	Little debate.
Biometric Identity Documents	Intense debate in U.S. with extensive consultation on biometric passports. Driving License standard rushed through on funding bill for Tsunami Relief.	Limited. Council ignored Parliament's concerns and called on Parliament to agree to demands or else Parliament would be removed from the process.

The above table shows that the situation in Europe is quite dire even as the U.S. Congress, Courts, non-governmental organisations, media and local governments work to minimise the harms and breadth of the anti-terror mechanisms introduced in the aftermath of September 11. Librarians protested loudly to oppose the Patriot Act even though no incursions took place under the powers that they were protesting against; media and civil liberties organisations exposed abuses; organisations pursued court cases; and public opinion polls showed declining support for expansive systems and policies. No similar moments of reconciliation have taken place at the EU to date as the Council of the European Union, the European Commission, and the various presidencies of the EU continue to push policies through there that break new grounds for surveillance and interferences with individual autonomy and fair processing.

In both contexts the worse policies go by when no one is looking. REAL ID and US-VISIT did not receive adequate attention and scrutiny in the U.S. as the Bush Administration moved to ensure that there was minimal debate. Meanwhile in Europe, just about every policy discussed above was rushed through hidden from the attention of parliamentarians, the media, and civil liberties organisations.

While the U.S. appears to be awakening, Europe continues its slumber.

What's Wrong with Europe?

One of the largest differences between the U.S. and European public discourses is the lack of adequate scrutiny of the police actions by the state. This was not always so; for instance in the 1980s there were public demonstrations in the Netherlands protesting against the census. In almost every country there was some mass movement protesting against surveillance and interferences with individual autonomy. But we have not seen such public concern lately against police powers in Europe; in fact most public demonstrations are usually in response to the actions of America.

There is a lack of public attention to civil liberties in Europe in response to the proposed policies. One possible explanation for this situation is the dual-role of international institutions in European political and legal life. On the one hand, international institutions such as the EU are used by Governments to pass policies that have failed in national parliaments, to only be brought home as 'international obligations'. On the other hand one of the few standardising international human rights obligations, the European Convention on Human Rights, is often regarded as an external treaty and not as part of the fabric of political discourse; and appealing to the courts on such matters tend to be beyond the capacity of European actors.

For instance, in the current debate in the UK on greater anti-terrorism powers we are told that the greatest civil liberty is the right to life; and that the European Convention on Human Rights is getting in the way of the Government's attempts to ensure that 'most basic civil liberty'. This is a dangerous logic. It is most dangerous because it creates a false conflict between the great UK Government as it tries to protect the lives of Britons and the weak ECHR that seeks to impose death and destruction upon Britain. And the public appears to believe it: polling data supports this fatalistic view. By implementing the ECHR into British law in 1998 under the Human Rights Act, politicians have created an external outlet for blame. On top of that, trying to find justice within the ECHR process requires going all the way to the European Court of Human Rights, in Strasbourg. This process takes much patience and funding.

A similar situation arises in the regulatory regime for protecting personal data. For a long time Europeans have mocked the Americans for lacking an appropriate privacy-protection regime; the EU has a strong regime in the 1995 Directive on the protection of personal data in both the public and private sectors, while the U.S. only has such a law protecting the use of personal information in the public sector. Consistent surveys of the American people show that the vast majority are concerned with the use of personal data by both industry and government, despite the simplistic explanation that is usually proffered that Americans fear only their Government and not abuse by the market.

In Europe there seems to be a complacency on the protection of personal data. There are no equivalent surveys of public opinion except for when a terrorism law is being discussed. There is little public discussion on privacy. Instead regulators are entrusted and references to the law are considered sufficient. When the EU moved to transform privacy rules in order to enable communications surveillance the response from the general public was relatively mute. Little debate occurred in the public domain because the decision was made at the EU and not in Member States, and also because the argument that prevailed in what little debate that was held was that if you have nothing to hide then you have nothing to fear. If such a proposal for indiscriminate surveillance was made in the U.S. there would be massive public outcry. To date the only significant outcry has emerged from what few non-governmental organisations there are, from some public regulators, the telecommunications industry and select European Parliamentarians.

There is no daily discussion of constitutional rights and values in European societies and this may be attributable to the fact that these are seen as alien concepts. Data protection rules appear EU-based and make us complacent even while we rely on the law and regulators to protect our interests; and civil liberties are hardly protected by the ECHR even as a false dichotomy is created to place blame on the ECHR whenever a Government wishes to introduce problematic laws.

What is most lacking in Europe is the culture of rights. In the U.S. there is certainly public support for problematic laws but there is also the public discussion on rights and safeguards, innumerable court cases brought against the Federal Government, laws introduced to minimise intrusions upon the private lives of individuals, and countless studies conducted to point out troubles and flaws. Towns have even passed ordinances calling for refusals to comply with Federal agents using powers under the USA-PATRIOT Act. The notion of a surveillance policy chilling free speech is of grave concern to U.S. organisations, industry, jurists, amongst others; and legal and political action ensues. The sum of all of these actions is the constitution of the open society: people acting in order to question Government policy. In the U.S. not only do the avenues for such questions exist, but you

have people pursuing them because of the culture of rights. In Europe there is a lack of such impetus to pursue these causes.

Of course this is a gross generalisation. In the UK there are public demonstrations against detention powers; Britons do feel as though there is something 'un-British' about ID cards, restrictions on *habeas corpus*, and other measures introduced recently. The French people tend to frown upon discriminatory policies. But there is no denying that there is a significant difference to the French and UK public responses to the French and UK Governments' policies than the U.S. public's response to the U.S. Government's policies, particularly if the policies apply to Americans. The volume and quality of the debate differ significantly.

A lack of culture

It is not enough to claim privacy as a constitutional right, as essential to democracy, and to leave it at that hoping that no further incursions will arise. No constitutional right, nor any moral right for that matter, is absolute. Without institutional support these rights are almost without meaning. Unless there are institutions that will call into question policy, whether they are the media, civil liberties organisations, opposition parties and others, then constitutional rights are at the mercy of the executive. But the effect is even more corrosive than merely establishing bad policy.

Within the European Convention on Human Rights, the right to privacy is 'balanced' against many other considerations, on the following condition developed by the European Court of Human Rights: intrusions on privacy must be considered necessary in a democratic society and thus they must be deemed proportionate.

Society's attitudes thus become the barometer of privacy as a fundamental right. What is 'proportionate' and 'reasonable' is unclear. There was a time when we thought that capital and corporal punishment were reasonable and proportionate when the crimes were severe enough or the public wanted vengeance, retribution, and entertainment. Generally, this is no longer the case. But there was also a time when we believed that national databases were problematic, that mass surveillance of communications was wrong because surveillance required individual suspicion. Yet we now see these systems and practices spreading.

When the EU established the biometric passport regulations in 2004, it was decided behind closed doors that all European citizens will have to submit their fingerprints in order to get a passport. These fingerprints will then be verified at border entry points in the EU and, probably, while abroad. This will lead to the collection of fingerprints of 450 million individuals. As Europeans grow more accustomed to submitting their fingerprints for access

to borders they are less likely to be offended when their own home governments require their fingerprints for more general purposes. Of course the U.S. will be to blame for some of this corrosion of our attitudes because the Bush Administration led the charge to begin fingerprinting all visitors. Governments around the world point to that practice to justify their own; most recently the UK Government argues that fingerprinting its residents and citizens is acceptable because after all the Americans are doing it under VISIT. Individuals must disclose their fingerprints or they may not enter borders or hospitals; though it begins with coercion eventually it may become commonplace.

Previously we collected fingerprints of criminals, or collected information on suspects; now European societies seems less obsessed with due process, and many argue that they are willing to forego liberty in the name of security. Some schools in the UK are collecting fingerprints from children when they borrow library books; the public outcry was again minimal and the privacy regulator even acquiesced to this collection. In the U.S. when a school began using radio-ID tags on students it was national and international news and the school was embarrassed into halting the programme. As a result in the U.S. students are learning that they must not be tagged; and U.S. society and thus U.S. law is likely to see such tagging in the future as 'disproportionate'. In the UK where fingerprinting is taking place in libraries, and across the EU where Governments will hold the fingerprints of all, though it is likely that though there may be initial resentment, with time this will be seen as acceptable, reasonable, and proportionate. And when even greater intrusions are incurred, the Courts will say that people were willing to accept fingerprinting in schools and at borders, so subsequent policies will be regarded as reasonable and proportionate.

Our global society is transforming, yet few are noticing. We are blind to these dynamics. And increasingly few have the capacity to do anything about it.

But comparative studies help. In depth and longitudinal looks at the lifetime of a terror policy will show that over time these policies are either abused or contained. If we may better understand the legal situation in other countries we are in a better position to deflate the rhetoric of some governments that argue that urgent action is absolutely necessary. If something is absolutely necessary in the war on terror we may ask questions such as:

> Why is it that it has failed elsewhere? e.g. ID cards in Spain did not prevent terrorist attacks;
>
> What are the legal ramifications? e.g. data mining projects in the U.S. were withdrawn on legal and technological grounds; and

Why has it been rejected elsewhere? e.g. the U.S. is not implementing retention of communications data.

While Governments insist on copying bad laws and outdoing one another with greater powers, they are not so eager to learn from what has been tried and failed elsewhere. Instead they endeavour to minimise debate and discussion, ignoring all input and the diversity of views. It is almost as though they believe that in order to save the Open Society, its principles must be trodden upon. These are precarious times for such a cavalier attitude particularly when there is so much at stake.