International cooperation became a key feature in politics with the growth of global communication networks and globalization of trade in the 1990s. After 9/11, international cooperation hit a new level, with all the major international bodies supporting cross-border anti-terrorism measures. Agreeing was so easy that governments increasingly have policies that are unpopular on the domestic front ratified at international gatherings, then re-introduce them at home, where they can be justified as fulfilling international standards. Civil society and democratic procedures meanwhile are left out of the picture entirely. The process has become known as "policy laundering" and has made inroads into daily life more than is generally known. An overview of the new political landscape.

Once, we dreamed the future and it worked: people and information flowed free and unchecked by borders or governments; the boundless possibilities of the latest technology harnessed to global welfare; the open society in which rights were protected and in which every citizen had the right to participate in making and shaping the nature of that society. We took it all for granted. What we actually have is something very different.

Immediately after the London bombings of 7 July, the UK government courageously fended off calls for additional legislation. On the following day, the home secretary went so far as to say that ID cards would not have prevented the attacks. However, while civil libertarians rested that weekend, the government was preparing a raft of policies to take to Brussels for an extraordinary meeting of the Council of Europe on Wednesday 13 July. The policies included calls for additional communications surveillance, fingerprints in ID cards, monitoring of financial transactions, increased information sharing and even a “name and shame” system for countries that refused to increase surveillance while reducing safeguards against abuse.

Rather than run the gauntlet of democratic procedures and submit themselves to the scrutiny of their citizens and fellow politicians, governments around the world are choosing to make their decisions behind the closed doors of ever more obscure international bodies where their citizens cannot enter and accountability is nil.
Discussion is kept to a minimum and contentious or controversial views are discouraged. The real work of government is now done at international organisations with their decisions handed down at summits in the form of press releases. Government by treaty and international agreement – without the whiff of a vote or smell of dissent. Those who would bring real debate to the table, notably industry and non-governmental organisations, are left outside.

As for the technology: it seems mainly to be in the service of these same governments which deploy it ever more widely in the surveillance and control of their citizens.

How did it all happen? How did democratic decision-making slide so quietly into the limbo of international consensus? How have we slipped so blindly into a surveillance society? It’s all about cooperation, stupid: it’s in fashion; everybody’s doing it. International cooperation is a good thing: we’ve always done it one form or another. And now there is the war on terror: the ultimate imperative in the internationalists’ armory – and the technology to make it possible.

This latest phase of cooperation began in the 1990s with the growth of global communications networks, increased globalisation of trade and movement and, some might argue, the triumph of the West as witnessed by its victory in the Cold War. In 2001, it reached new heights. In the days following 11 September, every international organisation stepped up to the plate with their demands for international co-operation. The United Nations responded with Resolution 1368 calling for increased cooperation between countries to prevent and suppress terrorism; NATO invoked Article 5 of its charter claiming an attack on any NATO member country was an attack on all; the Council of Europe condemned the attacks, appealed for solidarity and also called for increased cooperation in criminal matters; the Council of Europe Parliamentary Assembly later called on countries to swallow any reservations they had and ratify conventions combating terrorism as well as extending the mandate of police working groups. The European Union was quick to follow suit pushing for a European arrest warrant and common legislative frameworks for terrorism; it increased intelligence and police cooperation, froze assets and ensured the passage of the Money Laundering Directive. The OECD furthered its support for the Financial Action Task Force on Money Laundering and, along with the G7/8 and the European Commission, called for the extension of its mandate to combat terrorist financing. It looked to most like an entirely rational and logical response: terrorism is, after all, an international problem.

Ever since then, international organisations around the globe have been busy. The Asia-Pacific Economic Community may differ on trade policies but, year in, year out, declarations emerge calling for enhanced identity documents and travel surveillance. The Association of Southeast Asian Nations might disagree on how to deal with Burma, but are willing to share intelligence information within the region. G5 nations – Britain, France, Germany, Italy and Spain – might disagree on trade barriers and tariffs, but they meet frequently to agree on deportation, asylum and communications surveillance policies. Whenever the G8 meets, there is some expectation that tensions will flare between the US and France or Russia on issues dealing with Iraq or Iran, but we are never left in any doubt that each summit will finish with another declaration on surveillance of travel and communications, or the standardisation of identity documents. The Gulf Cooperation Council (GCC) meets yearly to call for the eradication of the “filth”
of terrorism and measures to regulate money laundering. In the Organisation of American States, Brazil and Mexico might complain to the US about new immigration practices that include fingerprinting all visitors; but peace reigns when the US department of state announces grants to fund the OAS for “the training of customs and border officials, to study ways to improve border management practices, and to support a comprehensive aviation security program”.

It became so easy to negotiate internationally on the things they all wanted, governments came to the conclusion that their summits would be an excellent conduit for the passage of domestic policy. Policies likely to meet fierce opposition at home, such as the recent attempts by the UK government to introduce ID cards, are now introduced into the domestic setting by the back door: agreed at an international gathering and returned home in the shape of a global standard that imposes domestic obligations. Now the UK is calling for biometric identity cards. This is a country that hasn’t had an identity card since the war-time card that was abandoned in 1952. But the government is now claiming that the US, the EU and international standards are forcing it to collect the fingerprints, iris scans and facial images of all Britons. It is hardly amusing that there are two faults in this line of reasoning: first, the international standards and obligations do not call for a vast database of the fingerprints and iris scans of all Britons; second, the UK government should know this because it was pushing for these standards at the EU and the UN.

This is how the UK justifies ID cards: most EU countries have ID cards, so why don’t we? Canada tried a similar approach by saying that 100 countries have ID cards, so why shouldn’t Canada? Similarly, in the heated debates of March 2005, when the UK government was calling for the power of house arrest, ministers pointed to other countries with similar laws and practices. Most of these countries have ID cards or detention without trial because these powers were created during more illiberal times. France’s national registration number and card, and detention authorised by investigative judges, dates from the Vichy regime. Both are alien to British history and law.

The self-referring circular nature of such arguments obfuscates the issues and keeps society at large in ignorance of the implications of the policies. Unsurprisingly, opposition from civil society is in retreat. The problem then becomes one of a lack of access and knowledge. Our conception of the open society relies on a local sovereign government making decisions through a clear and familiar process. This process permits actors to influence the decision-making process through lobbying, petitions, increased media awareness and so forth. These actors don’t customarily have access to international summits. Doors are closed only to be reopened for press conferences announcing the signing of treaties and declarations.

Using the analogy of money laundering, this process has come to be known as policy laundering. Much as dirty money is passed through a variety of legitimate enterprises to return circuitously but spotless into the owner’s account, so policy passes through international halls and returns home without benefit of due process.

The effect of this process on our daily lives is more draconian than we might realise. It is most intrusive in the invasion of our privacy via the web of surveillance that is stretching to encompass much of the globe. As we grow accustomed to generalised surveillance of
our activities online, we shall start to regulate our own conduct; if we know that our
Internet-service providers are keeping records on our activities for three years, we are
less likely to download controversial material. As the culture of rights dissipates, so do
our individual rights. And when we cannot identify the agencies, regulators or courts to
which we may appeal, which we are left without our rights. In our globalised world we
have yet to generate global accountability structures.

One of our most cherished assumptions in an open society is that we have the right to
free expression, particularly on the Internet. Tony Bunyan and Barry Steinhardt note that
the “surveillance society” is changing all that. Bunyan notes that governments are
pushing for the retention of “traffic data” at communications service providers. Once they
are compelled to keep the transaction logs of all our telephone calls and Internet use for
a number of years, we shall not feel free to express ourselves as we did. These measures
will have implications for freedom of expression.

A number of anti-terrorism laws introduced around the world involved curbing hate
speech. There are already many instances of countries announcing the “takedown” of
websites hosting “radical” Islamist material. In reaction to the assassination of a Dutch
film director, Belgium announced its intention to shut down certain Islamic web sites and
closely monitor radio programmes promoting violence. In reaction to threats made on
websites or the posting of messages from terrorists, websites have been removed or their
contents blocked. It is likely that the website visitation logs with the details of all visitors
to the particular server were also seized in the process; under data retention rules, this
information must be kept for years.

This problem will grow as countries ratify the Council of Europe Cybercrime Convention’s
Additional protocol on racist and xenophobic speech. This calls for the criminalisation of
the dissemination of threats and insults. As the Cybercrime Convention requires all
parties to the Convention to co-operate with one another in combating crime, the practice
of takedown, seizure, and surveillance of speech will spread across borders. One example
of what can already happen is the Indymedia case.

The Independent Media Center is an international news network of individuals,
independent and alternative media activists, and organisations. On 7 October last year,
its servers were seized from the London office of Rackspace, a server-hosting firm. The
loss of the servers resulted in the removal of content from 20 news websites. Rackspace
received a US court order to hand over the servers in London. According to the general
secretary of the National Union of Journalists in the UK: “To take away a server is like
taking away a broadcaster’s transmitter. It is simply incredible that American security
agents can just walk into a London office and remove equipment.”

The reason for the seizure remains under seal and no US law enforcement agency has
taken responsibility for the investigation into Indymedia; nor were any UK law
enforcement authorities involved in the seizure even though it took place in London. A
public prosecutor in Italy admitted that she did request the logs from the server, through
a request to the US authorities, on the grounds of combating terrorism. There was also
an unconfirmed request from the Swiss authorities. The US authorities responded to this
call for assistance, in compliance to international agreements, and approached Texas-
based Rackspace. Rackspace complied – even though its servers were in the UK.
This is the new face of censorship. Every action was in accordance with the law, but in a variety of jurisdictions. European governments argued that this was in accordance with their laws on terrorism; the US could successfully argue that they were merely adhering to international obligations; Rackspace could say that it was legally compelled to action by the US authorities; the UK could claim they had nothing to do with the seizure.

The only institution that has no direct claim on the law is Indymedia. To whom do they appeal? These operations were based in the UK, but no UK court will entertain a suit because there was no action in the UK. The US courts were forced into action when a motion was filed to get access to the subpoena used by the US government, but the subpoena was sealed and inaccessible. Legal action against European governments will require resources that Indymedia does not have access to.

Even legal recourse is often unavailable. Laws are increasingly being written to avoid disclosure and oversight as the USA-PATRIOT Act illustrates. Under the USA-PATRIOT Act, the Federal Bureau of Investigations may demand information from ISPs by showing a “national security letter”, without any judicial oversight. ISPs are required to comply but are not permitted to disclose their compliance. NSLs are issued without any judicial review, requirement to show individualised suspicion or compelling need, and cannot be contested. The American Civil Liberties Union challenged this procedure on many grounds including its infringement of First Amendment rights. In September 2004, a US district judge agreed:

The Court concludes that such First Amendment rights may be infringed [...] in a given case. For example, the FBI theoretically could issue to a political campaign’s computer system operator an [...] 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 [...] to discern the identity of someone whose anonymous online web log, or “blog”, is critical of the Government. [...] These prospects only highlight the potential danger of the FBI’s self-certification process and the absence of judicial oversight.

The Court also argued that “transactional records” deserve privacy protection, despite existing jurisprudence on telephone traffic and bank records that leaves Internet traffic data in legal limbo:

NSLs can potentially reveal far more than constitutionally-protected associational activity or anonymous speech. By revealing the websites on visits, the Government can learn, among many other potential examples, what books the subscriber enjoys reading or where a subscriber shops.

When the US ratifies the Cybercrime Convention, or when any government approves of the policy of communications data retention in accordance with EU policy, this problem will proliferate. And governments will tell courts they must comply in the name of international co-operation. Collaboration will spread beyond combating terrorism and into activities such as combating copyright piracy and other less serious crimes.
Our vision of an open society included the assumption that we can all participate in shaping national norms and laws. We believed that deliberative policy processes were the ideal fora in which we could lobby, raise our concerns and alert attention. With the very different dynamics of international policy, we are left with a significantly alien landscape; one that presents some serious challenges for anyone attempting to traverse it. Most notable among them are those that centre round the following:

**Government representation** It is increasingly clear that governments prefer to seek laws at international fora instead of having to deal with national deliberative processes. But those who represent them are frequently not representative of government at all: they can be anything from ministers of justice to senior civil servants who operate away from public scrutiny, the media and other government agencies and ministries. Deals on communications and travel surveillance, for instance, are not negotiated in tandem with ministries of commerce and trade; this leaves other arms of government powerless to question controversial policies. Even trade agreements are negotiated with little representation from other government agencies, as David Fewer suggests.

**Access and representation by civil society** Even if lobbyists, nongovernmental organisations, watchdogs and others were to become interested in international issues, they would be prevented from participating. And if one forum for general participation were to open up, governments would be quick to move serious decision-making to another, more secret one. The question of who should represent civil society is not entirely resolved by the multi-stakeholder initiative and, as Karen Banks points out, there is much still to be done if NGOs generally are to be as effective in the international arena as they have, in the past, been on the domestic front. This, necessarily, will involve the inclusion of some groups to the cost of others; yet when industry and civil society collaborate, the achievements can be significant.

**Better information** The policies that are laundered through international institutions are complex and subtle. We know very little about many of these, even less about the intricacies of these policies. Too few journalists, advocates, and even politicians know of organisations such as the GCC, the OSCE, APEC, ASEAN and other three- and four-letter organisations. On top of that, at first glance the policies all seem reasonable: access to airline reservations systems and communications data seem uncontroversial when combating terrorism; the collection of DNA of all those who are arrested seems reasonable; the protection of intellectual property in a globalised world to enable trade seems logical. Those who customarily question policies at the national level are not aware of the developments at international institutions. When governments bring these policies back home under the guise of an international obligation, few have sufficient information to question the nature of these “obligations”. Few know, for instance, that the ICAO standard on biometric passports does not require the collection of fingerprints, despite the claims of the UK government to the contrary. Even fewer understand the intricacies of DNA profiling and evidence as the Tania Simoncelli and Helen Wallace article indicates.

**Recourse and accountability** When policies are decided at the international
level, traditional structures for enforcement and accountability tend to be lacking. As Barry Steinhardt shows, even as it was demanding access to data that is protected under EU law, the US government was reluctant to grant Europeans the same rights of due process. The Indymedia case also shows that when international criminal investigations occur, it is difficult to pinpoint the source of the enquiry and the grounds for legal recourse.

**Openness and transparency** International fora are not renowned for openness. Access to information tends to be limited to public declarations after the event; we are not able to contribute to, or question the results. As the Steinhardt article notes, repeated attempts to gain access to the International Civil Aviation Organisation failed. When the Council of Europe established the Cybercrime Treaty, international NGOs who tried to influence the outcome of the treaty got the cold shoulder. Even where regulations on disclosure should, in theory, come into play, governments frequently claim exemption on the grounds that these do not apply to international negotiations.

It is not my intention to belabour the bleak landscape or give way to counsels of despair; international co-operation can be a positive force. World summits can play a positive role in generating interest, creating networks of support and influencing decision makers. International organisations do much to promote and protect human rights: governments model their human rights laws on those from other countries. Data protection laws are harmonised across the EU to promote privacy protection, just as freedom of information rules are modelled on those in other jurisdictions and further openness internationally. It is difficult to draw a broad stroke across these dynamics and label them evil; but when they are used to circumvent national processes and national law, it is a retrograde force – as the globalisation of surveillance most strikingly demonstrates.

It is important that we know what is happening and that we encourage debate on new strategies for the maintenance and enhancement of the open society. We must be wary of claims justified by “international obligations”, the need for “international cooperation” and calls for “harmonisation”. As long as governments fail to show the same eagerness for more progressive regulatory regimes – on global debt and the environment, for instance – we must question their zeal for collaboration in other areas.

Most important, we need to find ways to generate, sustain, and cultivate the culture of human rights. This will always remain the strongest defence against policies that threaten to diminish our individual or collective rights. Civil society also needs to cooperate internationally to find ways to do this; after all, so the logic goes, the world is going global and so must we.

**Published 25 October 2005**

Original in English
First published in Index on Censorship 3/2005
Downloaded from eurozine.com (https://www.eurozine.com/walking-on-the-dark-side/)
© Gus Hosein / Index on Censorship / Eurozine