



Barry Steinhardt

Three cheers for international cooperation

The US has often looked to Europe as a role model for how civil liberties should be protected. But three examples show that the Wild West legal regime is rubbing off on Europe. The Council of Europe Cybercrime Treaty, a US project that has been ratified by the minimum number of countries, will require international cooperation regardless of national laws. The monitoring of air passengers, a deal made between the US and the European Commission in 2003, will oblige data sharing that contravenes European privacy laws. And a bill requiring that nationals who do not need a visa to enter the US provide biometric information on passports is being reciprocated by the EU.

Organizations around the world involved in the fight to preserve civil liberties are increasingly confronted by an insidious new tactic: policy laundering. Policy laundering takes advantage of the fact that domestic institutions created to ensure democratic control and input into the policy-making process have not yet been extended to cover most international bodies. Nor have important institutions such as the press and public interest groups, which long ago figured out how to work within the domestic system of checks and balances, always adapted well when issues move to international forums.

When it comes to efforts to increase the surveillance of its citizens and others, the US, in particular, appears to be pursuing the strategy more or less consciously. Three examples of this trend include the Council of Europe Cybercrime Treaty; the effort to increase the monitoring of air passengers; and the push for global biometric identity documents.

The Council of Europe Cybercrime Treaty, purportedly an effort to improve international coordination in combating online crime, but actually far broader, was finalized in November 2001 and will go into effect this summer now that it has been ratified by the minimum number of signatories, mostly Central European nations. The convention was drafted by the then 43-member Council of Europe with the US, Canada, Japan, and other countries participating as "observers". In practice, the US was a major impetus behind the agreement.

Under cover of an unobjectionable banner — helping the police combat cybercrime — the treaty will also expand police search powers without corresponding privacy or due process protections, and require police in the US or Britain to cooperate with foreign police even when the behaviour under investigation is not actually illegal in either country.

It would be hard to find a clearer example of an attempt by the US government to gain new law enforcement powers through international channels that would

probably not be granted through the regular domestic political process. For example, the treaty, which was introduced at a time when controversy within the US over the FBI's Internet wiretapping device "Carnivore" was at a peak, would require the US to approve the use of such devices to capture the content of communications — a power it does not have clear authority for under US law. Unlike telephone wiretaps, which are set up by the telephone company on behalf of the authorities to listen to one line, Carnivore allows law enforcement agents direct access to ISPs' entire networks for surveillance, with only their unsupervised self-restraint preventing them from inspecting the vast flow of other data in the network.

Although internal disagreements within the Bush Administration appear to have slowed the treaty, it is moving steadily toward ratification. In November 2003, President George W. Bush sent the treaty to the Senate, and the Foreign Relations Committee began hearings in June 2004.

An example of another stripe of policy laundering can be seen in the Bush Administration's efforts to demand access to passenger-records data on Europeans flying to the US.

The US government's demands have run up against European privacy laws, which are far more comprehensive than anything in force in the US today. Like every advanced industrial democracy except the US, Europe has in place an overarching privacy directive that gives the force of law to a set of privacy principles that are recognized around the globe as core to the dignity and freedom necessary for a democratic citizenry. Unlike the primitive privacy protections that Americans still live under, European privacy law does not permit its citizens' personal information to be shared and traded willy-nilly by any corporation or government agency with a claim to a role in the war against terrorism.

Sadly, the US government's response to this conflict has been to bully and cajole the EU into betraying its own privacy laws. In fact, the Bush Administration is asking the Europeans for data-sharing on terms that go well beyond what is needed for the airline security purposes it claims to be pursuing, and well beyond anything directed by Congress.

After months of pressure, negotiators at the European Commission finally knuckled under to US demands and betrayed their own citizens' privacy interests. In December 2003, after extended negotiations, the European Commission announced that an agreement had been reached with the US. Under the agreement, the Europeans:

- declared US privacy protections "adequate", despite the fact that the US clearly does not meet the criteria for such a finding;
- accepted the US offer to retain European data for 3.5 years, far in excess of what EU regulations permit;
- allowed the US to use European information for regular crimes, even though the EU legal regime only permits data transfer for combating terrorism; and
- accepted a weak due process procedure that is entirely internal to the Department of Homeland Security, where EU rules require a true right to redress for citizens who believe their data is being abused.

Given its clear violation of EU requirements, the deal reached by the European Commission has been challenged by the European Parliament, which, in April 2004, passed a resolution asking the European Court of Justice to rule on whether the agreement violates European law. It remains unclear whether the Commission's deal can go into effect without parliament's approval.

Americans interested in protecting civil liberties have always seen Europe as a shining example of the kind of legal regime that we need to fight for here; but instead of Europe's civilized privacy regime rubbing off on the US, it appears that its Wild West legal regime is rubbing off on them.

Of course, as European critics have pointed out, the European Commission might have its own interests in weakening EU privacy standards: US and European governments might have been using each other to overcome the respective domestic obstacles each faced to an increase in the extension and rationalization of their own identity-tracking systems. And once again, the US government is embracing reciprocal arrangements; at the June 2004 G8 summit of major industrialized nations, Bush administration officials announced a new, reciprocal aviation-security plan under which personal data about US travellers would be shared with other nations, beginning with the G8 members but soon to expand to the rest of the world.

In addition to the above arrangements, under the New Transatlantic Agenda agreed to in Barcelona in 1995, the US and the EU are also cooperating through secret meetings such as the EU-US Task Force and the Senior Level Officials Group. The goal is to present common demands on such bodies as the International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO). Plans are also afoot to draft a multilateral accord among the 55 members of the Organization for Security and Cooperation in Europe (OSCE).

In the wake of the September 11 terrorist attacks on New York's Twin Towers, some in the US began to push for the creation of national identity cards. These efforts elicited a fierce backlash from Americans who did not want to see the creation of a tool that would inevitably be used to track and monitor average citizens. Once again, the Bush Administration turned to international forums. It prompted Congress to pass the Enhanced Border Security and Visa Entry Reform Act (EBSA) requiring allies of the US whose citizens do not need visas for entry into the US to begin including biometrics on their passports. Nations that failed to comply were threatened with losing their status as "visa-waiver" countries.

For the citizens of other nations, the US created a system called US VISIT, under which foreigners visiting the US would be fingerprinted and photographed, and their information stored in a biometric database for decades. It seems inevitable that foreign governments will reciprocate, with the result that Americans will find themselves treated in a similar way if they travel abroad. One nation, Brazil, reacted swiftly by putting similar measures into effect exclusively for US visitors.

Far from being concerned that such systems would lead to the retaliatory creation of systems for tracking Americans elsewhere in the world, administration officials have embraced such reciprocity. "We welcome other countries moving to this kind of system," Department of Homeland Security undersecretary Asa Hutchinson declared. "We fully expect that other countries

will adopt similar procedures."

The US assigned responsibility for the crucial question of exactly how biometric passports would be implemented to a heretofore obscure international group, the International Civil Aviation Organization, which is nominally sponsored by the UN and made up primarily of representatives of advanced industrial nations. ICAO developed these standards over a period of months in meetings held around the world. Despite repeated attempts by the American Civil Liberties Union, Privacy International, and others to gain access to these meetings, ICAO has rebuffed NGO attempts to provide input on the privacy implications of the particular standards being considered, or even to attend the meetings to a degree that would be impossible with a domestic decision-making body.

The resulting standards provide for the use of unreliable face-recognition biometric technology, as well as the inclusion of radio frequency identification (RFID) chips. The latter emit radio signals that can be used to read a passport holder's identity at a distance. A retail store or restaurant, for example, might gain the ability to capture the identities of those who walk through a portal; a government official could instantly sweep a room to discover who is attending a political meeting.

With its push for a biometric passport, the US government skipped right over proposals for a national ID card and focused on the international arena, where it set a course towards the creation of a global identity document or, at least, towards a set of global standards for identity that can be incorporated into a wide variety of national identity documents.

Such documents will increasingly be demanded for more and more purposes, not only around the world but domestically as well. Features such as the inclusion of a remotely readable RFID chip would greatly enhance the private sector's tendency to piggyback on the perceived "trust value" of these documents. There are justifiable fears that they might effectively become necessities — advancing the government's interest in tracking and controlling the movement of citizens and creating in the process a template for domestic National ID cards.

The "9/11 Commission" confirmed these suspicions: its influential final report approved the ICAO process, called for biometric travel documents, and wrote that "the international community arrives at international standards for the design of passports through the International Civil Aviation Organization". The report goes on to call for federal standards for the issue of driver's licences, declaring that "secure identification should begin in the United States".

Congress proceeded to do just that. In May 2005, Congress passed the Real ID Act that creates, in fact, a national ID system. It does so by mandating the standardization of the 50 states' driver's licenses and the interlinking of the databases that lie behind them, effectively taking what were state-issued documents originally intended merely to certify driving ability and turning them into federally controlled, fully fledged identity documents. The rules for these IDs are, as of this writing, being created by the Department of Homeland Security, an agency that has strongly supported the creation of the RFID-enabled passports and expressed interest in extending the technology from passports to the new driver's licences.

In short, policy laundering in the US has proved to be a highly successful strategy for the government to circumvent domestic opposition to national ID cards. In two and a half years, we have witnessed the push for ID cards come full circle from Homeland Security to ICAO to passports to domestic driver's licences; the evolution of travel surveillance that led to the transformation of EU law and practice reciprocated by the US; and we shall sooner or later see the collection of fingerprints and face scans just about everywhere we travel.

When it comes to policies that involve greater government surveillance and oversight of individuals, decision-making has shifted from the democratically accountable domestic arena to international structures that can operate in secret and in defiance of public scrutiny. If domestic organizations that have traditionally served as a countervailing influence against government surveillance are to continue to be effective, they must begin to adapt to the new reality.

Published 2005-10-25
Original in English
Contribution by Index on Censorship
First published in *Index on Censorship* 3/2005
© Barry Steinhardt/Index on Censorship
© Eurozine