

## **Problem of Policy Laundering**

Barry Steinhardt  
American Civil Liberties Union  
August 13, 2004

A new challenge has emerged in the democratic battle to preserve civil liberties in the United States and around the world. This challenge is what has been dubbed “policy laundering” – the use of foreign and international forums as an indirect means of pushing policies that might never win direct approval through the regular domestic political process. In a rapidly globalizing world, this technique is rapidly becoming a central means by which the United States (and other nations) seek to overcome civil liberties objections to privacy-invading policies.

Just as “money laundering” describes the cycling of illegitimate funds through outside institutions in order to enter them into legitimate circulation, so does policy laundering involve the cycling of policies that lack political legitimacy through outside institutions in order to bring them into circulation despite their lack of acceptance.

Policy laundering takes advantage of the fact that the institutions Americans have created for ensuring democratic control and input into the bureaucratic policymaking process have not yet grown to cover most international bodies. Every nation must reach a balance between direct democratic control over policymaking and the granting of discretionary freedom to its bureaucratic elites. In the United States, that balance was set through our Constitutional framework to include such elements as the creation of the legislative branch with its “power of the purse” and attendant oversight functions, and has been finely honed over time to include procedures such as public comment periods, open-meeting and open-records laws, and appeals processes of various stripes. In addition, other important institutions such as the press and public-interest groups long ago figured out how to work within this system.

Much of this democratic infrastructure has not yet been extended to international forums, however. Reporters, NGOs, and other important institutions such as Congressional Committees that are used to working on domestic issues do not always adapt well when consideration of those issues moves to international forums. Open-meetings rules and other rules that ensure accountability may be absent or impossible to enforce.

As a result, the Federal government is increasingly turning to international forums where those counterweights are not yet developed. The United States appears to be pursuing a more or less conscious strategy of policy laundering when it comes to efforts to increase the surveillance of its citizens as well as foreign nationals. Two examples of this trend include the push for global biometric identity documents, and the effort to increase the monitoring of air passengers. But the first most prominent example was the Council of Europe Cybercrime Treaty.

### **Cybercrime Treaty**

The ACLU received its introduction to policy laundering techniques via an instrument known as the Council of Europe Cybercrime Treaty. This agreement, 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, at least for the five small Central European Nations which have ratified it. The convention was drafted by the 43-member Council of Europe, with the U.S., Canada, Japan, and other countries participating as “observers,” although in actuality the United States was a major impetus behind the agreement.

Introduced at a time when domestic controversy over the FBI’s Internet wiretapping device “Carnivore” was at a peak, this treaty would require the United States to approve the use of such devices for purposes such as the interception of the content of communications, that have never been approved by the Congress.<sup>1</sup> Under cover of an unobjectionable banner – helping the police combat cybercrime – the treaty would also expand police search powers without ensuring corresponding privacy or due process protections, and require police in the United States to cooperate with foreign police even when the behavior under investigation is not actually illegal here.

It would be hard to find a clearer example of a government attempt to gain new law enforcement powers through international channels that would probably not be granted through the regular domestic political process.

Ironically, although the Cybercrime Treaty is perhaps the ultimate example of policy laundering, for unknown reasons the Bush Administration, and most of our major European allies are sending mixed signals about their willingness to have their nation’s bound by its terms. It. Despite a post-9/11 political environment that would have been favorable for passage, President Bush did not send the treaty to the U.S. Senate for ratification until November 2003, nearly two years after the United States signed it, and has not pressed for action. There was a brief hearing before the Senate Foreign Relations Committee in June, but no further action in the Senate.

Instead the US has pursued a different, more targeted form of policy laundering seeking bi-lateral or multi-lateral agreements on more discrete topics.

### **The push for a “global ID”**

In the wake of the September 11 terrorist attacks, some in the United States began to push for creation of National Identity cards. These efforts collided headlong, however, into 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.

So the Bush Administration turned to international forums. It prompted Congress to pass a law (the Enhanced Border Security and Visa Entry Reform Act, or EBSA) requiring our allies whose

---

<sup>1</sup> Unlike telephone wiretaps, which are set up by the telephone company on behalf 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.

citizens do not require visas to enter the U.S. to begin including biometrics on their passports, with the threat that any nations that failed to comply would lose their status as “visa-waiver” countries. For the citizens of other nations, the U.S. created a system called US VISIT, under which foreigners visiting this country would be fingerprinted and photographed, and their information stored in a biometric database for decades.

Neither of these measures are targeted at the U.S. population – at least directly. But many other nations appear to resent these measures, and foreign governments will inevitably reciprocate, with the result that Americans will find themselves similarly treated as they travel abroad. One nation, Brazil, in fact, reacted swiftly by putting similar measures into effect solely for their American visitors.<sup>2</sup>

Far from being concerned that such systems would lead to the retaliatory creation of systems for tracking Americans elsewhere in the world, Bush Administration officials have embraced such reciprocation. “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.”<sup>3</sup>

The United States 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 (ICAO), which is nominally sponsored by the United Nations, 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. The ACLU and Privacy International tried but failed to arrange attendance for a representative at a March 2004 meeting held in Cairo. An open letter to the ICAO on privacy concerns drafted by the ACLU and Privacy International, and signed by more than two dozen NGOs from around the world, met with no response.<sup>4</sup> The ACLU again wrote to ICAO asking to attend a May 2004 meeting in Montreal, and received no response.

In short, despite the importance of technical and interoperability standards, which can mean the difference between a use of biometrics that poses enormous problems for privacy, or one that poses little, ICAO has ignored attempts by privacy and civil liberties groups to join in their process. To a degree that would not be possible with a domestic government decision-making body, they have rebuffed NGO attempts to provide input on the privacy implications of the particular standards being considered, or even to simply attend the meetings.

The resulting standards provide for not only the use of the unreliable face-recognition biometric technology, which will result in many errors, but remarkably for the inclusion of Radio Frequency Identification Chips (RFID Chips) in all passports and other identity documents as well. RFID Chips emit radio signals that can be used to read a passport holder’s identity without

---

<sup>2</sup> See e.g. Kevin G. Hall, “Brazil ratifies fingerprinting, photographing of U.S. visitors,” Knight Ridder, Feb. 12, 2004; available online at <http://www.miami.com/mld/miamiherald/news/world/americas/7934565.htm>.

<sup>3</sup> Rachel L. Swarns, “Millions More Travelers to U.S. to Face Fingerprints and Photos,” *New York Times*, April 3, 2004.

<sup>4</sup> See ACLU et. al., “An Open Letter to the ICAO,” March 30, 2004; online at <http://www.aclu.org/Privacy/Privacy.cfm?ID=15341&c=130>.

his or her consent and 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, or a government agent could instantly sweep the room to discover who is attending a political meeting.

In short, skipping right over the politically untenable proposals for a National ID card, the U.S. government has embarked upon a course that will lead to the creation of a *global* identity document: the biometric passport. Once created, these passports will inevitably come to be seen as the gold standard of identity verification, either displacing driver's licenses, or becoming the model for new, more rigorous and standardized versions thereof. They will increasingly be demanded for more and more purposes, not only around the world, but domestically. Features such as the inclusion of a remotely readable RFID chip will greatly enhance the private sector's tendency to piggyback on the perceived "trust value" of these documents, which will turn them into necessities, which will in turn advance the government's aim of tracking and controlling the movement of its citizens.

Or innocent citizens, at any rate. As the perceived "trust value" of these documents rises, and as their adoption becomes more widespread, the payoff for counterfeiting them also rises – perhaps even more steeply – with the result that counterfeit or fraudulently acquired real documents will continue to remain available to determined and well-financed wrongdoers.<sup>5</sup>

### **Airline passenger data**

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 U.S. In part, these demands arise out of its efforts to implement an airline passenger profiling system known as CAPPS II (for Computer Assisted Passenger Prescreening System), which is built around a secret process of background checks and risk ratings for every person who flies. But the American government demands have run up against European privacy laws, which are far more comprehensive than anything in force in the U.S. today.

Like every advanced-industrial nation except the U.S., 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, our government's response to this conflict has been to bully and cajole the Europeans into betraying their 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 that go well beyond anything directed by Congress. The U.S. demands include:

---

<sup>5</sup> See James Moyer, "Security Document Theory White Paper," online at <http://www.cfp2004.org/spapers/moyer-sdt.pdf>.

- A broad array of information about each traveler, including information that under European law is classified as “sensitive” and cannot be shared;
- The right to retain data for 3.5 years;
- Broad forms of access to information, including the right to direct electronic access to airlines’ computer systems;
- Weak forms of due process for any Europeans who are mistakenly or unfairly targeted by the system.

After months of U.S. pressure, negotiators at the European Commission finally buckled under to American pressure and betrayed their own citizens’ privacy interests. After extended negotiations, the European Commission in December 2003 announced that an agreement had been reached with the U.S. Under the agreement, the Europeans:

- Declared U.S. privacy protections “adequate,” despite the fact that the U.S. clearly does not meet the criteria for such a finding.
- Allowed the U.S. to use European information for regular crimes, even though the E.U. legal regime only permits data transfer for combating terrorism.
- Accepted the U.S. offer to retain European data for 3.5 years, far in excess of what E.U. regulations permit.
- Accepted a weak due process procedure that is entirely internal to the Department of Homeland Security, where E.U. rules require a true right to redress for citizens who believe their data is being abused.
- Despite earlier assurances that the use of European data for CAPPS II was not being considered, allowed for European information to be used to develop the new passenger profiling system.

Given its clear violation of E.U. 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.

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; unfortunately, instead of the Europeans’ civilized privacy regime rubbing off on the U.S., it appears that our ‘Wild West’ legal regime is instead rubbing off on them.

Of course, as European critics have pointed out,<sup>6</sup> the European Commission may have its own interests in weakening E.U. privacy standards – that is, the American and European governments may have been using each other to overcome the domestic obstacles faced by each to an extension and rationalization of their own identity-tracking systems.

In addition to the U.S.-E.U. negotiations, working group meetings of the “G8” organization of advanced-industrial countries have begun to consider for the first time the creation of systems for routine background checks on every airline passenger. A draft was drawn up by the “Roma” (counter-terrorist and security agencies) and the “Lyon” group (law enforcement agencies)

---

<sup>6</sup> Privacy International, “Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection,” February 2004; online at <http://www.aclu.org/Privacy/Privacy.cfm?ID=14850&c=40>.

concerned with organized crime), for an international standard to be put to the ICAO. The U.S. and the European Union are also cooperating through secret meetings like the “E.U.-U.S. Task Force” and the “Senior Level Officials Group” under the New Transatlantic Agenda (agreed to in Barcelona in 1995). The goal is to present common demands on bodies like the 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).

The ACLU and European groups such as Privacy International have been working to penetrate this international process. We met with the European Commission negotiators, prepared a detailed report laying out how the E.U.-U.S. passenger-data agreement fell short of European privacy laws, and worked to bring the poor privacy practices of U.S. airlines to the attention of European officials through meetings and letters.

### **Conclusion -- An International Cooperation**

What the European passenger data and biometric passport cases tell us is that national policies are increasingly being made through international means. If the ACLU and other organizations that have traditionally served as a countweight against the government’s tendency to expand the tracking of citizens for administrative and security purposes are to continue to be effective, we must adapt to the new realities of policy laundering and global decision making. In our globalizing world, the levers of power are no longer the same, and decisions being made by obscure international groups – like ICAO – that can operate in secret and without public input may in some areas end up affecting our lives more than the decisions of our elected representatives in Congress.

Recently, we joined with Privacy International and State Watch -- the European Human Rights monitor -- in a joint project to monitor the use of policy laundering and the work of international forums like the ICAO, as well as to empower NGOs world wide to respond to these new challenges. (Our joint website [policylaundering.org](http://policylaundering.org) will soon be unveiled. Combining our experience and expertise will enable us to make public, encourage debate on, and influence the course of policies emanating from these intergovernmental fora in ways that are beyond the current scope of our individual capacities.

Below is a short description of the Project’s goals

There are **four** objectives to this collaborative project.

1. Research and gain access to information regarding the conduct of inter-governmental organizations.
2. Study and inform parliaments, publics, and media of the impacts of external laws and agreements on national policies.
3. Build capacity for national and local NGOs to address these issues in their countries.

4. Develop options for democratic governance at national, regional and international levels.