different TAKES

A Publication of the Population and Development Program at Hampshire College • No. 45 • Spring 2007

Control Freaks: "Homeland Security" and "Interoperability"

by Ben Hayes and Roch Tassé

A primary consequence of government responses to 9/11 has been the development of the homeland security industry. In 2006 the global security market is expected to be worth almost $60 billion. By 2015 it is expected to grow to as much as $170-250 billion, depending of course upon levels of global insecurity. The 2007 US Department of Homeland Security budget alone is over $34 billion, two thirds of which is allocated for border security.

Growth in the industry is assured by massive government contracts and generous subsidies for homeland security research and development. The US government has earmarked $25 billion for industry and academia for the period 2006-10 while the European Union (EU) has already allocated $2 billion to its "security research program" for 2007-14 (in addition to member state subsidies). Defense contractors dominate the homeland security market place; IT giants have also been quick to capitalize. In the US, the main players include *Lockheed Martin*, *Raytheon*, *Boeing*, *Northrop Grumman*, *Ericsson, Seisint, Accenture and Unisys*. In the EU, the likes of *Thales*, *EADS*, *Finmeccanica*, *Sagem* and the defense lobby group *ASD* are among those setting the agenda. Sixty percent of the pilot projects funded under the EU security research program for 2004-6 are led by defense sector companies.

Public concern for what critics have dubbed the "security-industrial complex" has so far been muted by the manufactured demand for technology to combat a host of modern-day threats, real and imagined. Nevertheless, informed analysis of the policy frameworks across the homeland security spectrum reveals "solutions" geared more toward to the control of populations than the protection of them. At the heart of this paradox is what industry and policymakers call "interoperability": the provision of seamlessly compatible government systems.

The brief tour of homeland security and interoperability that follows only touches on tangible developments in Europe and North America. It is important to recognize that money is also being thrown at the stuff of science fiction and state secrecy (nanotechnology and microwave crowd control, for example) and that many governments in the south and east are as enthusiastic as those in the north and west.

From the Battlefield to the Border

The EU is now "defended" from those fleeing poverty and destruction by a formidable apparatus that includes landmines placed along the Greek-Turkish border, gunboats and military aircraft patrolling the Mediterranean and the coast of West Africa, and trigger-happy border guards and barbed wire fences around the Spanish enclaves of Ceuta and Melilla in Morocco. A consortium led by *Dassault Aviation*, Europe's largest manufacturer of combat aircraft, is now being funded by the EU to facilitate the introduction of drone (pilot-less) surveillance planes to detect would be "illegal migrants" along its external borders.

In North America, the US Congress approved a bill just weeks prior to the November mid-term election authorizing construction of a fence along a third of the US border with Mexico. In addition, a $2.5 billion contract was allocated to *Boeing* for the deployment, over a three to six year period, of a "virtual fence" consisting of an array of sensors, motion detectors, infrared cameras, watchtowers and drone planes that will eventually stretch along both the Mexican and Canadian borders. The contract may ultimately be worth as much as $8 billion as the US moves to secure maritime borders as well. Blackhawk helicopters, Citation jet interceptors and Pilatus surveillance planes have begun patrolling strategic areas along the Canadian border and the US Coast Guard has been conducting

live-ammunition drills conducted in the Great Lakes in violation of a 90-year-old treaty that forbids weapons on the waterways.

From Immigration Control to Social Control

Integrated border control systems are as much about internal control as external security. "Biometrics," from the two Greek words for "life" and "measure," form the basis of new identification (ID) systems and a multi-billion dollar industry, particularly in the EU where it has been agreed that from 2007 people will have to have their fingerprints taken to get a passport. Consequently, after 100 years of only fingerprinting criminals, the majority of the EU's population will have been fingerprinted within a decade (they will also be carrying a "biometric" EU ID card if the UK government gets its wish). All refugees and illegal migrants in the EU have been fingerprinted since 2000 and, following the lead of the US VISIT program, all visa applicants will be fingerprinted as well (data will be retained whether or not their visa application is successful).

The drive for "interoperability" means this information will soon be held on interconnected police databases across Europe. In 2007 the European Commission will begin development of an "automated fingerprint identification system" and an "entry-exit" system to record all travel into and out of the EU. Police and intelligence services across Europe will have access to the fingerprint data and, by linking the EU visa information and border control systems, all "overstayers" and illegal "aliens" will be the subject of automatic EU-wide "alerts" (*de facto* arrest warrants). Already, teams of police and immigration officers in the UK are equipped with handheld fingerprint scanners to detect illegal migrants; gradually, the technology will be rolled out to police forces across Europe.

P/d population & development

The Population and Development Program
CLPP • Hampshire College • Amherst • MA 01002
413.559.5506 • http://popdev.hampshire.edu

The seeds for similar systems have been sown across the world. In 2004 the International Civil Aviation Organization (a UN body) agreed on an international standard for passports with globally interoperable face recognition systems and RDIF chips in which the "biometrics" (including fingerprints) are to be stored. The US VISIT system provides the foundations for the screening of everyone entering and leaving the country and the retention of profiles on each individual for up to 40 years. This system also relies heavily on biometric identifiers and all individuals entering the US (including Canadians and Americans returning to their country) will soon be required to have biometric identifiers on one sort of travel document or another (passports, smartcards or visas). Canada is preparing to implement a parallel but interoperable system and began field trials of electronic visas with biometric features in October 2006.

Police and security agencies in the US and EU can now also access the "passenger name records" (PNR) – up to 35 categories of personal data – on air travellers prior to their departure. The PNR includes personal details, financial information and even meal choices. In many cases, US authorities have direct access to passenger reservation databases in other countries; more privacy-conscious governments are insisting they be supplied only with the data on in-bound passengers. When implemented, the UK's "e-borders" scheme will provide check-in desks with discreet "green" signal for board, "orange" for persons to be subject to security checks, and "red" for wanted persons or known security risks.

"Interoperability" is not just about the "harmonization" of government systems, it is about the globalization of control. It is no coincidence that since 2000 the US has provided the technology and funding for immigration control systems in more than 20 countries, including Afghanistan, Cambodia, Ethiopia, Ghana, Kenya, Pakistan, Tanzania and the Yemen.

Policing the Suspect Community

In the wake of 9/11, governments have demanded more and more information on their citizens, from telephone to library records. Under EU rules, all telecommunications traffic data in Europe must now be retained by telephone and internet service providers for law enforcement access. In the UK, where the police used to need a warrant to access an individual's call records, now all they need is a phone number. In Canada, Parliament was about to adopt "lawful access" legislation when it was dissolved for the January 2006 election. The bill

called for mandatory intercept capability on the part of telecommunication service providers and for warrantless access to customer data by law enforcement agencies. Security agencies continue to call for those measures and a new bill is expected shortly.

In August 2006 a US Federal Court ruled unconstitutional the President's self-declared power to authorize the National Security Agency to spy, without warrants, on e-mails, faxes and telephone calls going into and out of the country. That ruling is presently under appeal. North of the border, the very same warrantless interception powers are granted to the Communication Security Agency by Canada's Anti-Terrorism Act. The NSA controversy followed revelations in May that the agency has been secretly collecting the phone records of tens of millions of Americans, using data provided voluntarily by *AT&T*, *Verizon* and *BellSouth*. That same month, the Attorney General and the FBI Director also called on telecom companies to store data about users' activities for two years. The US government has also just been found guilty of unlawful surveillance of "SWIFT," a global bank transfers system based in Belgium, and is formally accused of violating privacy in over 30 countries. The EU, meanwhile, is quietly funding IT companies to equip its security services to do the very same thing.

"Inter-operability" is not just about the "harmonization" of government systems, it is about the globalization of control.

The UK "children's index" will potentially monitor every child from birth, including schooling, contact with health and social services, and even "problem" parents. The "Safeguarding Vulnerable Groups Bill," meanwhile, will mean that one third of the adult working population will be subject to ongoing criminal checks. A new UK national health database will centralize people's histories of mental illness, alcoholism, drug-taking, HIV status, pregnancy and other potentially prejudicial information. The police and security services and a host of medical professionals will have access to the database, prompting widespread fears about data security. No less alarming is the fact that everyone arrested by the UK police now has their DNA taken (even if subsequently they are not charged with any offense). The UK DNA database already covers one in every 20 people in the UK, a figure that rises to one in five black males. The EU and the G8 are both developing systems for the automated exchange and matching of DNA profiles.

Outside Europe, it is private corporations rather than governments that are at the forefront of collecting data on populations. This data is then being sold on the open market. Contracting out with data aggregating companies allows US government agencies to access and mine massive databases of personal information they would not, under privacy and other laws, be able to maintain themselves. The USA Patriot Act also gave the FBI broader access to records held by all American companies. This applies to the personal information on Canadians whose data is increasingly managed by American companies and/or their subsidiaries.

Full-Spectrum Dominance

Another key area into which homeland security funds are being ploughed is satellite monitoring systems. The EU's "Galileo" system is being developed on the much lauded premise of providing the world with its first non-military global positioning system. However, two-thirds of the financing for the current deployment stage of the satellites has now been provided by a consortium of Europe's biggest arms and aerospace companies. They hope to recoup their investment in a market for satellite navigation applications that could grow to a staggering $350 billion by 2020.

A predictable U-turn on the restriction of the use of Galileo to non-military purposes has now been signaled by the European Commission and a plethora of applications under development. This includes the "road pricing system" much vaunted by the UK government that would replace road tax with a "pay-as-you-drive" scheme in which every car journey would then be tracked and monitored by satellite.

The US, of course, already has its eyes in the skies. Its satellite imaging capabilities have been used to support its allegations that Iraq and Iran are developing WMD while the notorious "Echelon" surveillance system monitors global satellite and communications traffic.

In Defense of Freedom and Democracy

In the post-9/11 world, people who use the terms "police state" and "social control" are easily dismissed as conspiracy theorists. But as a "theory of conspiracy," these developments are entirely logical. In a world that takes no meaningful action

to address environmental catastrophe or the separation of the world's peoples into extremes of rich and poor, "full-spectrum dominance" over dwindling resources and resistant populations makes sense from both a risk management and a military perspective. And while governments and corporations drag their feet on climate change, their risk aversion and military strategies already stretch decades into the future.

Richard Thomas, UK Privacy Commissioner, warned recently that we need to wake up to the reality of the "surveillance society." What he did not say is what George Orwell understood perfectly well: a surveillance society is not a democratic society. In the latter, the government is accountable to the people; in the former, the people are accountable to the government.

These developments are as chilling as the fears they purport to address. But there are encouraging signs that people are waking up to the need to address the root causes of social problems, to defend their fundamental rights and take back power from governments and corporations. Just as a peaceful world would emasculate the military-industrial complex, a just one would render impotent the security-industrial complex.

Ben Hayes *is a London-based researcher with* Statewatch *and joint coordinator of the* European Civil Liberties Network. ***Roch Tassé*** *is coordinator of the Ottawa-based* International Civil Liberties Monitoring Group.

References

On the "Homeland Security" industry, see:

Ben Hayes, "Arming Big Brother: the EU's Security Research programme" (Statewatch/TNI, April 2006), http://www.statewatch.org/news/2006/apr/bigbrother.pdf.

Jay Stanley, "The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society" (ACLU, August 2004), http://www.aclu.org/FilesPDFs/surveillance_report.pdf.

On civil liberties and surveillance issues, see:

ACLU, http://www.aclu.org.

Statewatch, http://www.statewatch.org.

Privacy International, http://www.privacyinternational.org.

Electronic Frontiers Foundation, http://www.eff.org/Privacy.

On the militarization of border controls, see:

Frances Webber, "Border Wars and Asylum Crimes," Statewatch, 2006.

On ID cards, see:

Electronic Privacy Information Centre, http://www.epic.org/privacy/id_cards.

NO2ID, http://www.no2id.net.

On travel surveillance and profiling, see:

Privacy International, "Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection," (February 2004), http://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf.

The Practical Nomad, Edward Hasbrouck's blog: "Privacy and Travel" archives,

http://www.hasbrouck.org/blog/archives/cat_privacy_and_travel.html.

On telecommunications surveillance, see:

European Digital Rights Initiative, http://www.edri.org/issues/privacy/dataretention.

On global surveillance, see:

Maureen Webb, *Illusions of Security: Global Surveillance and Democracy in the Post- 9/11 World* (San Francisco: City Lights, publication forthcoming, January 2007).