## Surveillance and the War on Terrorism
## What's in a name?

- Jim Harper
Friday, October 15, 2004

Ask any CEO about the power of branding, and you'll get an earful. Most corporate chiefs would give anything to have the positive brand recognition of a Coke, a Kodak or a Google.

The architects of the surveillance state are using brand management, too, but with precisely the opposite purpose: to escape negative recognition. A case in point is a provision in an intelligence reform bill that passed the Senate last week. It calls for a "trusted" government surveillance network.

Few have forgotten the Defense Department's doomed surveillance proposal, Total Information Awareness. It would have comprehensively scanned the commercial activities and communications of all Americans in an attempt to weed out terrorists. It was lamely rebranded "Terrorism Information Awareness" before Congress terminated the program.

But Total Information Awareness may not stay dead all that long. The Senate intelligence bill, now being reconciled with similar House legislation, calls for a new "trusted information environment." The bill is, at best, ambiguous about how widely it would sweep as it conscripts privately held data for surveillance purposes.

Of course, Congress cannot decree that such a network will be "trusted." That is up to the American people. If government investigators are going to put citizens' eBay listings and credit-card records in the same pool as information about Hamas leaders, one doubts that trust will be forthcoming. And calling this surveillance network an "environment" will not make it more palatable either.

The idea for a "trusted" information network comes from a group assembled by the Markle Foundation, a New York nonprofit, that articulated such a program late last year. The group has tried to grab the high ground by painting opponents of comprehensive surveillance as anti-technology Luddites. Defending Total Information Awareness, the Markle group said, "We are disappointed that Congress found it necessary to ban research and development of technologies that would make use of privately held data."

But searching privately held data without a warrant is not a technology: It is a policy, and a bad one. The Markle group has analyzed the federal laws that control government access to private-sector information, a road map of sorts for law changes that will fold private data even further into national surveillance.

If there is to be a network, the mission should define the network, rather than the network defining the mission. Let there be networked delivery of warrants dealing with particular suspects, and networked responses to those warrants. Using technology consistent with the Constitution is perfectly acceptable, and there is no need for new legal authority if a network serves an existing legitimate purpose. But any technology that promises something "better" than law enforcement consistent with the Constitution -- well, that's just not better.

The rebranding of government surveillance programs continues with CAPPS II, the Computer Assisted Passenger Pre-Screening System -- now called "Secure Flight." The Transportation Security Administration put together this intrusive traveler background-check system to fight a crucial battle in the war on terrorism, but one that has probably passed as the terrorists move to new techniques. CAPPS II fell under the weight of congressional scrutiny when it abjectly failed to provide adequate protections for due process, privacy and other interests, as found by a Government Accountability Office study.

When he announced the supposed end of CAPPS II, Secretary of Homeland Security Tom Ridge joked about putting a dagger through its heart. Even a wooden stake, garlic and holy water would not have worked, unfortunately, because his foe is far more resilient than any vampire or zombie. CAPPS III/Secure Flight is up and walking around. It will soon be tested using data commandeered from the airlines regarding everyone who traveled domestically during June 2004. CAPPS III shares many hallmarks of the failed CAPPS II, though little information about the program is available yet. Foremost, Privacy Act protections will not apply, due to a law enforcement/national security exception to the act. This treats every American who flew domestically during June 2004 as a terrorism suspect. Travelers will not be allowed to decline participation.

The CAPPS III/Secure Flight program places no limits on how long data will be retained. Mission creep will inevitably lead the program to maintain records of Americans' travels well beyond the time when there is a legitimate terrorism-prevention purpose.

Finally, CAPPS III will use data compiled by commercial data aggregators in ways that have yet to be defined. This is an end run around the Privacy Act that deserves debate before federal agencies assume it is acceptable. Renaming CAPPS II "Secure Flight" does not change or make its avoidance of the Privacy Act acceptable.

Some consumer data companies, retailers and Internet companies may view the government surveillance market as a good one for them. They should think twice. The companies that sell data to government for this purpose, and the companies that sell data to those companies, may find themselves needing to re- brand because of public revulsion at the practice.

*Jim Harper is director of Information Policy Studies at the Cato Institute (www.cato.org).*

Page B - 11
URL: http://sfgate.com/cgi-bin/article.cgi?
file=/chronicle/archive/2004/10/15/EDGAB99A971.DTL