Senate Judiciary Committee Hearing
January 10, 2007
"Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs"

Questions re Testimony of James Jay Carafano

Question 1, Bullet 1:

1. **In your written testimony, you suggest several "guidelines" for government data-mining programs. Among other things, you recommend that, "[t]o protect individual privacy, any disclosure of a person's identity should require a judge's approval."**

    - **Would this restriction apply to disclosures from one government agency to another? If, for example, the Department of Defense conducts a data-mining program that yields three or four names of suspected terrorists that might be worthy of follow-up investigation, would you require the DOD to get a court order before sharing that information with the FBI?**

No, I am not recommending that information disclosures among departments or agencies within the federal government require a judge's approval. But at this relatively early stage in the federal government's development and implementation of data-mining technology to predict and prevent terrorist activity, personally identifiable information of an individual who has been identified as a terrorism suspect based solely on data-mining technology should not be disclosed to parties outside of the U.S. government without court involvement. Until the federal government has more experience using data-mining technology for predictive or preventative purposes, the U.S. government should not share such information with, for example, foreign governments to identify persons who should be restricted from travel or private financial institutions that are providing voluntary assistance in terrorist finance investigations.

This restriction against sharing personally identifiable information with parties outside of the U.S. government should not apply, however, if the suspicion of terrorist activity has an independent basis in information obtained using sources or methods other than data-mining technology. Thus, if data-mining technology merely provided the first indication that a person might be involved in terrorist activity, or if the information obtained using data-mining technology merely supports other information obtained using other sources and methods, then the fact that some information was obtained using data-mining technology should not be enough to require court involvement.

Question 1, Bullet 2:

- **Would you likewise require a judge's involvement before the FBI could share a name gleaned through data-mining with state or local law enforcement officers for further investigation?**

At this relatively early stage in the federal government's development and implementation of data-mining technology to predict and prevent terrorist activity, disclosure to state and local law enforcement officials should require some level of court involvement. I recommend that for now many of the same standards should govern disclosures to state and local law enforcement officials in the U.S. as are applied to disclosures to foreign governments and to private parties; however, a more relaxed standard of proof should apply to disclosures to state and local law enforcement officials in the U.S. as long as the person is merely being investigated and not subjected to a Fourth Amendment search or seizure. (See answer to following question.)

Question 1, Bullet 3:

- **If so, what standard of proof would apply? Would you require, for instance, probable cause to believe the identified person is involved in terrorism, even if the person is not going to be arrested or subjected to a Fourth Amendment search?**

I would not recommend that the same standard of proof be required for disclosure to state and local law enforcement officials in the U.S. as should be applied to disclosures to officials of other governments or to private parties. At this time, the judicially created reasonable suspicion standard, or a standard similar to it, is all that should be required for the federal government to disclose to state and local law enforcement officials in the U.S. personally identifiable information about an individual suspected of terrorist activity based solely on predictive data-mining technology.

Question 2:

2. **Your proposed "guidelines" for government data-mining programs include the suggestion that "[t]he federal government's use of data-mining technology should be strictly limited to national security-related investigations." Presumably this restriction would only apply to pattern-based data-mining used for predictive or preventative purposes?**

Correct. My recommendation should have noted that data-mining technology is already in use, with little actual controversy, by organizations in both the public and private sectors to identify patterns of existing fraudulent or otherwise criminal conduct. I am by no means recommending that non-predictive, non-preventative uses of data-mining technology such as these be restricted to national security-related investigations only.