Everything's Political

Write a mock policy memo about a contemporary topic of interest

Policy is everywhere: from the humanities to science. Even if you don't plan on working in Washington D.C. during your career you will likely need to confront a policy issue that will effect your work. Science funding, civil rights issues, the relationships between the federal government and big business, national security implications and even just simple tax issues will inevitably become relevant to you.

Often in academia you are praised for the ability to go on and on about a topic of interest. In Washington D.C. you will be fired for not getting to the point. If you are working on an issue in Washington, your superiors will often ask for your recommendation on a complex issue. It is up to you to do the research, succinctly describe the dilemma and your recommendation, and then send it in for a quick briefing by someone who has the power to implement change. Usually you are expected to send the memo ahead of time and then briefly present on the topic to answer questions. Here you will just write a mock memo on a policy issue of your choice.

To complete the skill module:

1) Go read the news and find an area affected by policy that's aligned with your interests. (Examples include stem cell research, academic funding, privacy issues, net neutrality controversies, etc.)
2) Select a government agency that makes decisions relevant to that issue (White House, Pentagon, FDA, NSF, etc.) and find a high ranking official you want to make your point to.
3) Do research on the topic to form a cohesive background and gather enough information to make an informed recommendation.
4) Write up a mock memo with your research and recommendation formatted similarly to an example I did for a policy class but feel free to find your own style of memo.
5) Send it to elainesedenberg@mail.utexas.edu for approval or contact me if you have any questions.

Memo

To: Duane Blackburn (OSTP) and Chris Miles (DHS S&T)
Chairs for the National Science and Technology Council Subcommittee on Biometrics and Identity Management

From: Elaine Sedenberg, University of Texas at Austin

Issue: The ability to quickly and correctly identify individuals who pose a threat to national security remains a constant challenge to our nation. Developments in technology have enabled the use of biometrics as a form of identification. The implemented use of biometrics as a form of identity verification comes with civil liberty debates and concern for the security of this information. Additionally proper use of biometrics will require controlled interoperability from various federal agencies.

General Background: Technology, such as the recently implemented full body scanners, allow more thorough security checks and give more information about individuals passing through checkpoints. The standard combination of an ID badge and mug shot as a means of identification have remained largely unchanged for decades. The introduction of biometrics offer novel ways of establishing identity and provides ways in which older standards such as fingerprints may be verified quickly and on the spot.

Biometrics are measurable biological characteristics that are unique to each individual. Biometric modalities include fingerprints, iris or pupil recognition, facial recognition, hand geometry analysis, and voice recognition. Each characteristic involves different levels of interaction from individuals (for instance facial recognition could be done by surveillance while fingerprinting requires cooperation) and each feature has different advantages and disadvantages.

The collection of biometric information from citizens and foreign individuals entering the country has raised many civil liberty questions. Aside from the actual acquisition of this personal data, there is concern about how surveillance may infringe on individual's right to privacy in the future. Additionally databases of this information must be unquestionably secure.

Recent Background: The NSTC Subcommittee on Biometrics was formed to provide leadership for the development and implementation of interoperable federal biometric systems. The committee was designed to adopt biometric standards and design multi-agency strategies.

In June 2008 President Bush released a National Security Presidential Directive and Homeland Security Presidential Directive to establish a framework for biometric data collection. This directive supported interoperability of agency systems for

suspected threats to national security. Only small progress has been made on this front since the directives.

Program Examples Utilizing Biometric Technology

Program	Agency	Contractor	Year Initiated	Brief Description
IDENT-IAFIS	DHS/DOJ		2004	10 print biometric ID at every U.S. Customs and Border Patrol station. Allows immediate background checks.
Registered Traveler	DHS	Various contractors	2004	For a fee individuals could get a background check and gain faster access through airport security checkpoints. Pilot program was completed. Several of the contractors have gone bankrupt.
TWIC	DHS	Lockheed Martin	2007	Controlled access and verified identification of maritime workers
NGI	FBI	Lockheed Martin	2008	Project to build a massive identification system to increase collection of multiple biometrics

Importance: Recent attempted terrorist attacks have illustrated the importance of seamless interoperability among the intelligence community. Scientifically biometrics have been established as proven methods of identification. Though the U.S. government has begun to implement these technologies, standards and information sharing among agencies have not been fully developed or executed. Though biometrics have repeatedly been emphasized, much of the implementation has not occurred.

Discussion: The Obama administration continues to make national security a high priority. Advances in technology which enable biometrics have made methods faster, cheaper, and more reliable. The nation is currently faced with an imminent paradigm shift in identity management. Photo IDs, which inherently come with the risk of fraudulent behavior, can be circumvented by combinational biometric data. Personal biometrics are difficult to alter and may provide instant background check access.

Programs which have already been implemented have shown limited success. Different agencies have taken project implementation upon themselves which has limited the projects' scope. Throughout the War on Terror, military personnel were able to collect biometric data from captured terrorist suspects and confirm their identities. This data acquisition has not been completely coordinated. The data acquired and submitted was left up to personal discretion on the field and without

standard procedure (sometimes both fingerprints and iris scans were collected, sometimes only one). Lack of interagency access to newly acquired data has also contributed to more alleged "stove piping" among intelligence agencies.

Similarly the Registered Traveler Program saw limited success but took strides towards implementing biometrics into airport security. Project implementation was done by multiple private contractors and was initiated in the midst of several other failed/cancelled airport programs. While the pilot program reached completion, this project was alarmingly fragmented.

Immediate Strategic Recommendations: Several prominent action recommendations are presented to the subcommittee for consideration. All recommendations are in line with the sub-committee's goals to tackle and coordinate our nation's use of biometrics.

A. Continue to make interoperability among agencies the top priority of the subcommittee and work towards setting a more definite strategic plan in place soon.

B. To further the development and adoption of biometric standards, the committee should consider making specific recommendations to agencies currently implementing biometric identification techniques. The committee should provide feedback on compliance with current standards and suggestions for improved methodology.

C. Streamline any further implementation of biometrics in airports and examine the security of data shared and monitored with contracted agencies.

D. Ensure proper security measures are explored for any national databases of biometric information. Leakage of information from any agency would prove disastrous.

Further Considerations: Implementation of biometric systems may be expensive but costs will not only be minimized in the long term (less personnel needed at checkpoints for example) but many agencies already own the equipment necessary. Most the challenges that should be immediately addressed by the committee are more organizational than technical.

Additional considerations should be made for civil liberties. Recently (March 30, 2010) a recommendation was made to President Obama seeking nomination of members to the Privacy and Civil Liberties Oversight Board. It is advisable to allow this Privacy Board to oversee civil liberty issues while our committee should continue to monitor standards and structural policies.

By addressing these areas, the subcommittee may further advance our nation's implementation of biometrics to improve national security and also address issues that have arisen from past projects.

References:

"Biometric Identifiers." *Electronic Privacy Information Center*. Epic.org, Web. 12 Apr 2010. <http://epic.org/privacy/biometrics/>.

"Biometrics.gov." NSTC Subcommittee on Biometrics. Web. 12 Apr 2010. <http://www.biometrics.gov/default.aspx>.

"The Biometric Consortium." Web. 12 Apr 2010. <http://www.biometrics.org/>.

Jaindl, Kimberly. "New Workstation Delivery Marks First Operational Milestone for NGI System." *Lockheed Martin* (2010): Web. 14 Apr 2010. <http://www.lockheedmartin.com/news/press_releases/2010/0106_lockheed-delivers-ngi-atw.html>.

Magnuson, Stew. "Defense Department Under Pressure to Share Biometric Data." *National Defense Magazine* (2009): Web. 12 Apr 2010.

"Presidential Directive." *NSPD-59/HSPD-24* . N.p., 05 June 2008. Web. 12 Apr 2010. <http://www.biometrics.gov/PresidentialDirectives/Default.aspx>.

"TSA News Ticker." *TSA Registered Traveler*. TSA, 15 July 2009. Web. 14 Apr 2010. <http://www.tsa.gov/approach/rt/index.shtm>.