

Privacy Advisory Committee
Wednesday, August 18, 2004, 1:30 p.m.
House Room D, General Assembly Building
Richmond, Virginia

The Privacy Advisory Committee, charged with reviewing current privacy laws and practices as they pertain to information and its treatment both in cyberspace and physical space, met for the second time on August 18, 2004. The Committee also is charged with proposing policies and guidelines for public bodies to evaluate the use of potentially invasive technologies when determining whether to support their use financially or to authorize or prohibit their use. During this meeting, the Committee continued discussing the use and misuse of modern technologies and began discussing the privacy of personally information.

Facial Recognition Technology

Greg Mullen, Deputy Chief of Police, City of Virginia Beach, briefed the Committee on the City of Virginia Beach's process for implementing facial recognition technology. Residents throughout the Hampton Roads area and several million tourists visit the Virginia Beach oceanfront. To maintain the Virginia Beach Police Department's commitment to the safety and security of these tourists and residents, the city added facial recognition technology to the existing closed circuit television video camera system during the summer of 2002. Until that point, Tampa was the only other jurisdiction to use it.

Prior to implementing the technology, the Department researched it for several years beginning in 1999. Facial recognition technology is a biometric application that converts an image (e.g., a mug shot or photograph) into a mathematical algorithm that a computer can use to compare that image to another one. The Department developed a dynamic database of pictures and biographical data on people that meet specific criteria. The cameras scan locations where people frequent attempting to match images of those people with images in the database. Police Department tests of the system, which are conducted annually, show an 84 to 85 percent accuracy rate. Tests during all light conditions, show an accuracy rate in the mid-70 to mid-8-percent range.

Above all else, the Department believed that full disclosure was paramount to implementing a successful program. Using a grant from the Department of Criminal Justice Services, the Department set out to involve the community and let them know that the Department was not trying to hide anything. It initiated a media and communication campaign to disclose what the technology can do, why the Department was implementing it, and how it would be deployed. News releases, media interviews and a city website helped the Department reach out to educate the community by dispelling myths and spreading facts.

After fully disclosing its intentions and conducting the research, the Department began an education campaign, first by briefing city leaders on the potential for using the technology and then by educating the public. The Department briefed the City's Human Rights Commission to learn of issues that might affect citizens and worked with interested groups including civic organizations, business communities, boards and commissions.

To foster public input, the Police Department held a town hall meeting on the technology and streamed the meeting on the Department's website to provide greater access. During this meeting, a panel of experts in privacy, law enforcement, business and research - the President of the Virginia ACLU, a Rand researcher, the Police Chief, a representative from the business community, a representative from the Tampa Business Community Advisory Board, and a civil rights lawyer - answered questions from the public. In addition to televising the meeting, the Department also advertised the issues and answers to the questions on the website and through the local newspaper.

To maximize public knowledge and input, the Department publicized its effort through interviews with local and national television stations, conducted one-on-one briefings with council members to address all the issues and possible problem areas, and held a public hearing with the council prior to a vote. When Council made the decision to implement the system, the Department held a news conference to inform everyone and reinforce its commitment to ensuring that the program was operated in a manner that balanced law enforcement's needs and those of the community. The Department held another new conference once the system was operational and provided demonstrations, allowing the media to film use of the system in process to verify that the Department is doing what it said it would do.

In addition, the Department formed the Facial Recognition Technology Citizen's Advisory and Audit Committee. Because the Department believed that it was important for the group to reflect the community, it included representatives from the NAACP, Hispanic Dialog, Human Rights Coalition, the local Philipino community, and other human rights and minority groups. The Committee exists to oversee and assist in the preparation and implementation of the policies and procedures that govern the Department's program.

Together, the Department and the Committee developed specific criteria for the type of people who would be in the database and the policies for operating the system. First, people with outstanding felony warrants (about 650) were loaded into the database. Later, the group added lost or missing children, runaways, other missing persons, the Top 20 Terrorists and the FBI's Top 10 Most Wanted. Finally, law enforcement officials can request that a specific individual be added for a specified, limited time. The database would not store images from the cameras and would be reviewed daily and updated accordingly. To limit privacy concerns, the data would not be stored and the system would not be connected to outside databases or the Internet.

Using an algorithm that contains 80 points of the face, the technology avoids bias and stereotype. The closed circuit television video feed, which is saved for seven days, sends images to the system for comparison. A match creates an alert. The system then sends the image and the top ten closest matches from the database to an officer for comparison. The system only saves the image if the officer verifies the match and prints the image. Then, the Department will dispatch an officer for a voluntary encounter according to its standard operating procedures.

To protect the citizens, the Department must have policies for everyone using the technology. A police officer audits the system monthly and a private citizen group audits it quarterly through random audits to ensure compliance with the policy and maintain the integrity of the system.

Civil Rights groups also have uninhibited access to audit the system and report on its progress. The system is not used unless trained officers are present. The Department provided schedules of use to the audit committee so that they can audit it when it is operational.

The Department's use of facial recognition technology is publicized throughout the area with signs warning people and cameras located in plain sight. The Department received a \$200,000 grant to purchase and install the equipment, train officers in its use and maintain it for three years. The system replaced the manned surveillance cameras that were typically used during events and holidays. The Department also used cameras to videotape arrests to protect police and suspects. It needed something better and less expensive to identify and prevent problems and deter crimes in the area. The Department enhanced its current infrastructure and built a scaleable system. In the two years that it has been running, there have been no complaints and no arrests. According to Deputy Chief Mullen, the area is one of the safest in the Commonwealth and his Department wants it to stay that way.

After the presentation and questions, the Committee discussed other uses of such a system. Currently, Arizona and Florida are using this technology at their Department of Motor Vehicles Offices and jails. In addition, they connected their system more systems than Virginia Beach. Senator Watkins cautioned that private entities can take photographs without most privacy issues and at some point, run them through this type of system. Deputy Chief Mullen responded that the Las Vegas casinos do this now. He reminded the Committee that facial recognition technology is just another tool to increase the chance for apprehending wanted people, deterring crime and saving runaways. Even a 50 percent chance (the Department of Defense accuracy rate) is better than no chance at all.

Legislative Proposals

Turning from technology to information, the Committee discussed legislative proposals from the 2004 Regular Session. The House Committee on Science and Technology continued the first (House Bill 753). The General Assembly enacted the second with a reenactment clause (House Bill 543). The patron redrafted the third proposal before its introduction and ultimate passage (House Bill 1424). The requestor of the last proposal never introduced it; the Committee discussed it with that person's approval (notice of breach of system).

Display of Social Security Numbers - Private Sector

The House Committee on Science and Technology (HCST) considered and carried over HB 753 (Patron - May), a JCOTS recommendation, which would have limited the use of social security numbers in the private sector. The bill would have amended the Personal Information Privacy Act to protect the social security number from public display and insecure transmission. The bill would have allowed those who use the number prior to the effective date of the bill to continue using it so long as the use was continuous if the user provided to the number holder an annual disclosure and a cost-free opportunity to discontinue use.

The bill also would have required that insurance plans for state employees assign an identification number that is not a covered employee's social security number. Finally, the bill

would have amended the Virginia Consumer Protection Act to prohibit a supplier from using a consumer's social security number when the consumer requests that his driver's license number be used. Current law requires that a supplier only provide an alternate number if the consumer so requests in writing. This bill provides consumers with another option other than providing their social security numbers and writing to the supplier for a new number.

Use of Social Security Numbers - Public Records

During the 2004 Regular Session, the General Assembly passed HB 543 (Patron - May), a JCOTS recommendation, with a reenactment clause. The bill would have prohibited filing or creating public records that contain more than the last four digits of any unique identifying number, unless such use is required by law or the record is exempt from disclosure. The bill defined unique identifying number as any alphabetic or numeric sequence, or combination thereof, that is unique and assigned to a specific natural person at that person's request and includes, but is not limited to, social security number, bank account number, credit card number, military service number and driver's license number. The bill excludes from the definition any unique identifying number that an agency assigns to a natural person in place of a social security number for identification so long as it is used for a single, specific government purpose. Either preparers or filers of such documents would have to certify that the document complies with this prohibition before the documents could be filed. Because the enactment contains a reenactment clause, the 2005 Session of the General Assembly must reenact the provisions of the bill for it to become effective.

This measure limits the appearance of key identifiers for access to financial records, medical records and other similar records as a means of addressing both privacy and identity theft concerns.

Personal Identification Information on Negotiable Instruments

The General Assembly passed HB 1424 (Patron - Dudley), which prohibits a person who accepts checks in the transaction of business from recording a date of birth upon the check as a condition of accepting the check. The section does not affect collection of a birth date for reasons unrelated to accepting the check, nor does it block a requirement that the payor provide his year of birth. This proposal is a natural extension of that bill and restricts the use of personal information that can be used to commit financial fraud and identity theft on all negotiable instruments. This measure limits the use of key information for access to financial records as a means of addressing both privacy and identity theft concerns.

Notice of Breach of Information Systems

This measure would require any state agency or business that owns or licenses a computerized database that includes personal information to disclose a breach of the security of that system to any resident of the Commonwealth whose unencrypted personal information may have been acquired by an unauthorized person. This proposal was not introduced during the 2004 Session, but was discussed with the approval of the legislator proposing it.