Privacy Advisory Committee
Wednesday, July 7, 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 on July 7, 2004. The Committee is also 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 reviewed the use of various types of technologies.

Potentially Invasive Technologies
House Bill 1304 (Lingamfelter)

During the 2004 Regular Session, the House Committee on Science and Technology (HCST) considered and carried over bills that would have required (i) public bodies to conduct a privacy impact analysis when authorizing or prohibiting the use of invasive technologies (HB 1304) and (ii) manufacturers of vehicles equipped with recording devices to disclose that fact in the owner's manual (HB 697). HCST referred these bills to JCOTS for study.

Delegate L. Scott Lingamfelter (Patron - HB 1304) explained that HB 1304 would have required public bodies to conduct a privacy impact analysis when authorizing or prohibiting the use of invasive technologies (e.g., radio frequency identification, tracking systems, facial recognition systems, hidden cameras, spyware, photo monitoring systems and Internet wiretaps) beginning July 1, 2006. The bill also would have required JCOTS to propose to the Governor and the General Assembly policies and guidelines for public bodies to follow in conducting the privacy impact analysis. In developing the policies and guidelines, the bill required JCOTS to review the invasive technologies available for use, the current legal requirements of their use and the reasons for their use, their impact on civil liberties, and any safeguards that are or should be used to mitigate negative impacts.

Del. Lingamfelter said that he introduced the bill because he realized that while the legislature has been asked to authorize, limit or prohibit the use of many new technologies such as facial recognition and photo monitoring systems, the needs of legitimate law enforcement must be balanced against the preservation of the American way of life and our inalienable freedoms. He understood that the development of new technologies has challenged the balance between civil liberties and security, a long-established principle embedded in the constitutions of the United States and the Commonwealth of Virginia. Technologies available today can track a person's movement, listen to his conversations, assess the speed of his vehicle and look inside his house all from a remote location and without his knowledge. As they become more invasive and their use more clandestine, the potential for unchecked abuse threatens to impinge civil liberties. Therefore, Del. Lingamfelter found it crucial to have more information when deciding on legislation that affects their use.

Event Data Recorders
House Bill 697 (Morgan)

On behalf of Delegate Harvey Morgan (Patron - HB 697), Mitchell Goldstein, Executive Director and Chief Counsel, JCOTS, briefed the Committee on HB 697, which would have required a manufacturer of a new motor vehicle sold or leased in the Commonwealth that is equipped with one or more recording devices, commonly referred to as "event data recorders" (EDR) or "sensing and diagnostic modules" (SDM), to disclose that fact in the owner's manual for the vehicle. The bill would have prohibited specified data that is recorded on one of these devices from being downloaded or otherwise retrieved by a person other than the registered owner of the motor vehicle, except under specified circumstances. The bill also would have required a subscription service agreement to disclose that specified information may be recorded or transmitted as part of the subscription service.

Robert J. Breitenbach, Director, Transportation Safety Training Center, Virginia Commonwealth University, provided an overview of the history and use of EDRs. On June 10, 1997, the National Transportation Safety Board (NTSB) adopted a series of new recommendations on air bags and automobile occupant restraint use. The recommendations arose from the NTSB's public forum convened in March 1997. One of the recommendations the NTSB made to the National Highway Traffic Safety Administration was to "develop and implement, in conjunction with the domestic and international automobile manufacturers, a plan to gather better information on crash pulses and other crash parameters in actual crashes, utilizing current or augmented crash sensing and recording devices." In response to this recommendation, domestic automobile manufacturers began introducing "EDR" functionality in its current form in vehicles for model year 1997. However, EDRs were first introduced in model year 1990 vehicles that were equipped with air bags and only recorded very limited data.

EDRs made by different manufacturers record different data. However, most EDRs record whether the driver's and passenger's seat beats were buckled or unbuckled, whether the air bag engaged, engine speed, vehicle speed, and whether the brake switch was on or off. The devices begin recording vehicle data when the device detects the vehicle slowing down along its length with enough force to cause the module's crash sensing algorithm to 'wake up' and anticipate a collision severity which warrants an actual deployment for that vehicle. Technicians can download information from the devices either using the vehicle's diagnostic link connector (DLC), which is installed under the dashboard on all vehicles from 1996 or later or directly from the air bag module located under the passenger's front seat.

Mr. Breitenbach illustrated six sets of crash data for the Committee, using each set to highlight different aspects of EDR data as it is used in analyzing automobile crashes. In addition to the data collected by EDRs, crash reconstructionists collect and analyze real world data, such as acceleration/distance analysis and speed determination. The real world data is often gleaned from physical evidence, including skid marks and a thorough examination of the crash site and the automobiles involved. In each set of crash data, the data recorded by the EDR was generally consistent with the physical evidence observed and the reconstruction analysis. Some crash situations may make the EDR data inconsistent with physical evidence, such as when a vehicle

goes airborne or a wheel breaks from its axle. In these cases if the accelerator is continuously applied there may be spikes in engine speed and vehicle speed.

Mr. Breitenbach emphasized that the EDR is a tool to be used by the crash reconstructionist, not a replacement for them. The device supplements good investigative and analytical procedures. It does not stand alone in many real world events; a full analysis of the crash is still required.

In spite of the value of the data recorded by EDRs, significant privacy concerns surround these devices. Most notably, EDR data is relatively easy to retrieve, requiring only a small investment in hardware (several thousand dollars at most), working knowledge of the software, and access to a vehicle containing an EDR. The information, while gathered to enhance safety in motor vehicles, can be used to determine fault in the event of a crash, whether the driver wore a seat belt and potentially even driving habits.

Radio Frequency Identification

Bradley Canel, Manager, Accenture Technology Labs, briefed the Committee on radio frequency identification (RFID). RFID is a generic term for technologies that use radio waves to automatically identify people or objects. RFID uses several methods of identification, but the most common is storing a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification information to a reader. The reader then converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it.

An RFID system consists of a tag, which consists of a microchip with an antenna, and an interrogator or reader with an antenna. The reader sends out electromagnetic waves. The tag antenna is tuned to receive these waves. A passive RFID tag draws power from the field created by the reader and uses it to power the microchip’s circuits. The chip then modulates the waves that the tag sends back to the reader and the reader converts the new waves into digital data. Active RFID tags have a battery, which runs the microchip's circuitry to broadcast a signal to a reader (the way a cell phone transmits signals to a base station). Passive tags have no battery. Active and semi-passive tags are useful for tracking high-value goods that need to be scanned over long ranges, such as railway cars on a track. They cost a dollar or more each, making them too expensive to put on low-cost items. Companies are focusing on passive tags, which cost approximately 25 cents each when purchased in volumes of 1 million tags or more. Their read range is not as far -- typically less than 20 feet as opposed to 100 feet or more for active tags -- but they are far less expensive than active tags and can be disposed of with the product packaging. Passive tags have considerable benefits, particularly in retail inventory applications.

RFID tags differ from the traditional bar code technology because they do not require line of sight. They can be read as long as they are within range of a reader. Bar code scanners must be near a scanner that can "see" the bar code to read it, which means people usually have to orient the bar code towards a scanner for it to be read. If a bar code label is ripped, soiled or falls off, there is no way to scan the item. RFID codes are long enough that every RFID tag may have a

unique code, while UPC codes are limited to a single code for all instances of a particular product. The uniqueness of RFID tags means that a product may be individually tracked as it moves down the supply chain. This may help companies to combat theft and other forms of product loss. RFID tags enabling everything from tracking cows and pets to triggering equipment down oil wells. The most common applications are tracking goods in the supply chain, reusable containers, high value tools and other assets, and parts moving to a manufacturing production line. RFID is also used for security (including controlling access to buildings and networks) and payment systems that let customers pay for items without using cash.

The use of RFID technology has generated considerable controversy and even product boycotts. The four main privacy concerns regarding RFID are (i) the purchaser of an item will not necessarily be aware of the presence of the tag or be able to remove it; (ii) the tag can be read at a distance without the knowledge of the individual; (iii) if a tagged item is paid for by credit card or in conjunction with use of a loyalty card, then it would be possible to tie the unique ID of that item to the identity of the purchaser; and (iv) tags create, or are proposed to create, globally unique serial numbers for all products, even though this creates privacy problems and is completely unnecessary for most applications.

Most concerns revolve around the fact that RFID tags affixed to products remain functional even after the products have been purchased and taken home, and thus can be used for surveillance, and other purposes unrelated to their supply chain inventory functions. Although RFID tags are only officially intended for short-distance use, they can be interrogated from greater distances by anyone with a high-gain antenna, potentially allowing the contents of a house to be scanned at a distance. Even short range scanning is a concern if all the items detected are logged in a database every time a person passes a reader, or if it is done for nefarious reasons (e.g., a mugger using a hand-held scanner to obtain an instant assessment of the wealth of potential victims). With permanent RFID serial numbers, an item leaks unexpected information about a person even after disposal; for example, items that are resold, or given away, enable mapping of a person's social network.

Mr. Canel emphasized that radio frequency technology by itself is not invasive, but how the technology is employed to track objects may be. When asked whether an RFID tag embedded in a garment that is stolen could be read when the garment is worn into another RFID-enabled area, he replied that the present state of radio frequency technology does not permit ubiquitous radio frequency reading. He encouraged the Committee to keep three considerations in mind when addressing RFID issues: (1) the range at which the RFID tag can be read, (2) the purpose for which the RFID tag is being used, and (3) how access to and control of the information contained in the RFID tag will be managed.

Tracking Technologies for 9-1-1

Steve Marzolf, Public Safety Communications Coordinator, Virginia Information Technologies Agency, explained the tracking technologies used by the Commonwealth to help locate 9-1-1 callers whether from wireline or wireless phones. Wireline phones provide the registered name, physical address, telephone number, and class of service (residential, business, etc.) for all callers

to 9-1-1 operators. The call center can manually look-up this information by telephone number, if necessary. Additionally, information is available for exigent circumstances even if 9-1-1 not called.

Wireless phones provide two phases of information for callers to 9-1-1. Phase I provides a call back number and the address of the cell site processing the call. Phase II provides the Phase I data as well as the longitude and latitude for the caller with the accuracy being dependent on the technology. The accuracy of the Phase II location data can be addressed either through a handset-based solution or a network-based solution. The handset-based solution requires a global positioning system (GPS) in each handset; older handsets would have to be replaced and activated. This technology can provide an accurate location to within 50 meters of the phone on 67 percent of the calls, and 150 meters on 95 percent of the calls. The network-based solution triangulates the phone's location based on at least three cell sites. It works with existing handsets, but requires involving the carrier of the cell phone's signal. This technology can provide an accurate location to within 100 meters of the phone on 67 percent of the calls and 300 meters on 95 percent of the calls.

In addition to using telephony to locate 9-1-1 callers, 9-1-1 call centers also have access to multiple mapping and geographic information systems (GIS) databases, including digital aerial photography, assessment and property owner data, building photographs and plans and previous incident history. Future technologies may be able to track any type of communications whether through computers (telematics) or voice over Internet protocol (VoIP). Telematics may provide transmission of collision data to 9-1-1 center from an EDR, which would potentially assist emergency workers in determining an appropriate level of response. VoIP is an increasingly popular means of telephone service; however, 9-1-1 call centers receiving such a call need the ability to track the caller's location via the Internet and then route the call to the appropriate 9-1-1 center.

Use of this data is governed by the Wireless Communications and Public Safety Act of 1999 (WCPSA - 47 U.S.C. § 222) and the Communications Assistance for Law Enforcement Act of 1994 (CALEA). The WCPSA protects subscriber and location information and provides an exception “solely for purposes of assisting in the delivery of emergency services in response to an emergency.” This law allows access to subscriber information for emergency notification systems. CALEA requires a court order for other subscriber and location information. All 9-1-1 lines are recorded, and those recordings are public information subject to freedom of information laws.

Spyware

Brian Tretick, Technology and Security Risk Services, Ernst & Young, briefed the Committee on spyware. The term "spy" is misleading because even some of the most annoying software does not actually send any information back to a server or another third party, though it does retrieve information. Computer security people tend to call it all "malware," meaning it is harmful software. Some people distinguish "adware" (advertising-supported software that displays pop-up advertisements whenever the program is running) from "real spyware," such as Trojan horses (a destructive program that masquerades as a benign application) and keyloggers (programs that

record every keystroke and transmit the information to a third party). Typically, spyware arrives bundled with freeware or shareware, through email or instant message, or by someone with access to a user's computer.

It is often easier to define the bad things that should be avoided, rather than all the good things that should be allowed. Some of the bad things occurring today include software acting in unfair or deceptive ways, such as hijacking the computer or network resources; modifying the computer, network or other software or their configurations; and snooping, capturing data, or otherwise surveilling the computer, network, or other software. This includes use of email, instant messaging, Internet browsing, and even word processors. However, legitimate software may operate and have functions that the user is unaware of. Some current practices include targeting ads in exchange for some other benefit, such as special offers; monitoring and analyzing behavior; troubleshooting, error calculating and error reporting; and grid computing, using idle time to process a larger problem.

To get rid of the "spy" in spyware, industry and legislators must focus on transparency and other control by the user. Software must provide clear, conspicuous and accurate notice to the user; a consent requirement, involving informed consent; and the ability to disable and configure the software. Software should not provide a "silent back channel" communication or ET "phone home" features without notice to and control of the user or collect more information than necessary. Legislation must not eliminate legitimate, ad-supported software.

More information on Spyware

Spyware refers to executable programs placed on a computer, usually without permission or knowledge, that monitor or access information and report it to a third party. The programs can record keystrokes, take screen shots, scan files, install other programs, or monitor systems, providing access to passwords, credit cards numbers, and other sensitive information -- and even the ability to control the computer -- all without the user's knowledge, even if the user is not connected to the Internet.

Spyware can compromise critical information, lead to loss of intellectual property or other competitive advantage, and cause compliance issues as governments pass stringent laws to protect medical, financial and other sensitive data. They can violate privacy, detract from the computer's usability and stability, appropriate resources and even alter functionality.

A computer user can acquire spyware by clicking on deceptive pop-ups or links in e-mail, visiting certain websites that may require a plug-in, as a piggyback to a download or any number of other ways. Sometimes, the user unknowingly gives permission to receive the spyware by agreeing to, though not necessarily reading, a lengthy end user license agreement while downloading software.

Commonly-used security measures have proved inadequate to stop these programs. Firewalls operate on the boundary of networks and cannot detect spyware that is introduced from or is already running within the network. Anti-virus software typically does not detect spyware. Not

even encryption can stop it because keystroke loggers record keystrokes before the information ever is encrypted.

Software companies have developed programs to detect, disable, intercept or remove spyware, though they are of limited value. Some spyware vendors use techniques to avoid detection and removal, such as counterattacking the software in an attempt to disable it. Other programs use routines to re-install themselves after detection and deletion, or can defeat attempts to cut off their communication.

The best ways to stop spyware is to stop (or stop employees from) visiting websites known to distribute it and downloading applications that are infected with it. Computer users can install and operate intrusion detection software to alert them if anyone is trying to hack into their systems or send information through the Internet. Finally, setting the Web browser's security level to high and monitoring for and installing updates and security patches will better protect computer users. If all else fails, users must back up data in case their files are corrupted or destroyed.