County of Fairfax, Virginia

MEMORANDUM

DATE: APR 23 2015

TO: Board of Supervisors

FROM: Edward L. Long, Jr.
County Executive

SUBJECT: Policies Covering Collection and Retention of Electronic Data

In a January 13, 2015, Board Matter, staff was directed to provide the Board a recommended policy to govern the County's use of technology that collects sensitive data, as well as the use, possession, and retention of the data collected. The use of license plate readers was of particular interest to the Board. This memorandum provides a preliminary response to that request.

As the Board is aware, the subject of privacy has been of interest to the General Assembly in recent years, and this year was no exception. **HB 1673** (Anderson) and **SB 965** (Petersen), as passed by the General Assembly, address license plate readers as well as other types of surveillance technology, and would limit the use of such technology to collect or maintain personal information, in the absence of a warrant, when the collection of this information is not tied to a specific purpose, such as a criminal investigation. The bills would authorize the collection of information from license plate readers, but limit the retention of such data to seven days, unless it is being used in an investigation.

On March 27, Governor McAuliffe's amendments to the bills were released. The amendments proposed to limit the application of the bill to license plate readers and provide for a 60-day data retention period. The General Assembly considered these amendments at the Reconvened Session on April 15. As discussed in the update provided to the Board on April 17, the General Assembly returned the bills to the Governor in different postures. The Senate did not take up the Governor's amendments, returning the bill to the Governor as it passed the General Assembly. In contrast, the House rejected the expanded data retention period, but accepted the amendments limiting the application of the legislation to license plate readers. The Governor will thus have the choice of signing the original version, signing a modified version, or vetoing both bills. The Governor now has 30 days to act on the bills, or to allow them to become law without his signature. Therefore, it is likely that final action on this legislation will not occur until mid-May.

Office of the County Executive
12000 Government Center Parkway
Suite 552
Phone: (703) 324-2531, TTY 711
Fax: (703) 324-3956
www.fairfaxcounty.gov

Since state law would set the overall parameters of data collection and retention in this area, staff believes it would be prudent to delay a final response to the Board on this question until the Governor completes his work on this legislation. Note that County agencies must follow a number of state and federal statutes, regulations, and policies governing the collection and retention of data. For the Board's information, this memorandum provides a brief discussion of the County's overall data security policy and the Commonwealth's Record Retention Schedules. Statutes and policies specific to law enforcement will be discussed in more detail in the forthcoming update to this memorandum.

The Fairfax County Information Technology Security Policy (IT Security Policy) provides overarching guidance to County agencies regarding implementation and acceptable use of information technology including access, solutions, communications, and data. As stated in the IT Security Policy, all County agencies, employees and contractors are required to abide by all applicable laws, regulations, policies, and standards of conduct when using County information technology and communications systems, and, indeed, when handling County data in any format. To that end, all Fairfax County information systems that transmit, receive, process, and store information must be protected accordingly. In order to remain relevant as the laws, guidelines, regulations, and statutes regarding the use of technology and data evolve, the County policy is written broadly. County agencies may elect to go further within the requirements provided by the general County policy, by developing an agency-based policy that includes further details associated with specific operational needs for that agency. The IT Security Policy is comprehensive and can be viewed at: http://fairfaxnet.fairfaxcounty.gov/Dept/DIT/Information%20Security/pol_PM70-05_01.pdf. Please contact Chief Technology Officer Wanda Gibson if you would like more information about the IT Security Policy and DIT electronic data storage provisions.

There are many federal and state statutes and regulations governing privacy, security, and/or data retention. Examples include the federal Health Insurance Portability and Accountability Act (HIPAA); the Virginia Government Data Collection and Dissemination Practices Act; the Virginia Public Records Act; and the Virginia Freedom of Information Act. These are also referenced in the IT Security Policy.

In addition the General Assembly has authorized the Library of Virginia to establish the Virginia Records Retention Schedules which govern the retention and disposition of state and local public records (*Code of Virginia* § 42.1-85). These schedules are complex and the policies apply to multiple departments at both the local and state level. The current record retention schedules governing local law enforcement records, including license plate reader data, are available at: http://www.lva.virginia.gov/agencies/records/sched_local/GS-17.pdf. All 28 comprehensive retention schedules governing local government records are available at: http://www.lva.virginia.gov/agencies/records/sched_local/index.htm. Please contact Assistant County Attorney Sarah Hensley if you have legal questions regarding the existing record retention schedules.

Finally, the IT Security Office is responsible for the IT Security Policy as well as awareness and compliance. DIT and IT Security Office staffs work with County agencies when deploying any new technology to help assess risks and protect data. The County's IT Security Policy has been recognized as a best practice by public and private sector organizations that have broad knowledge of IT security programs for local governments.

Staff will be monitoring the Governor's final action on legislation and will provide updates to the Board as needed. Please contact Legislative Director Claudia Arko with any legislative questions.

A more detailed memorandum will be forthcoming after the state legislative process for 2015 has concluded. Let us know if you would like a follow-up meeting scheduled at your office about any topic in this memo.

cc: David P. Bobzien, County Attorney
David M. Rohrer, Deputy County Executive
David J. Molchany, Deputy County Executive
Edwin C. Roessler, Chief of Police
Claudia Arko, Legislative Director
Wanda M. Gibson, Chief Technology Officer
Gail P. Langham, Deputy County Attorney
Sarah A. Hensley, Assistant County Attorney
Bob Blakely, FCPD Sully District Station Commander
Gordon S. Jarratt, Director, Enterprise Systems Division

8b. **SETTING A POLICY FOR COLLECTION AND RETENTION OF ELECTRONIC DATA** (12:16 p.m.)

MOLCHANY/BOBZIEN/ROHRER/ARKO

Jointly with Supervisor Hyland and Supervisor Foust, Supervisor Cook noted that technology has brought to all levels of government the ability to collect and retain significant amounts and types of electronic data. Locally, the use of license plate readers can be used for such beneficial tasks as locating suspected criminals or analyzing travel patterns, and tracking the location of cell phones as part of police surveillance operations.

The County uses license plate readers. Last year a local newspaper reported on the issue of police collection of cell phone location data, but the County has not publicly confirmed whether it possesses or uses such technology.

Technology that tracks the location of vehicles and cell phones can provide powerful benefits to law enforcement and urban planners. However, it also raises significant civil liberty concerns. Such data could allow the government to track the daily movements of innocent residents without warrant or any showing of probable cause or public benefit.

While people may disagree on whether local government should even possess or use such technology, and if so under what rules, Supervisor Cook said he hoped what can be agreed on today is that it is the responsibility of the Board, the elected body of the County, to set these guidelines and procedures. It should not be left to individual departments to establish their own polices, but the Board has not yet spoken on these issues.

Therefore, Supervisor Cook moved that the Board direct the County Executive to provide to the Board, within 90 days, a recommended policy which would govern the County's use of technology that collects sensitive data as well as the use, possession and retention of the data collected. Supervisor Foust and Supervisor Hyland jointly seconded the motion.

Discussion ensued regarding the motion, and whether there is an existing State guideline already in place or whether it is on the agenda for the upcoming General Assembly session.

Supervisor McKay said that County Legislative staff will review upcoming bills before the General Assembly and report to the Board.

The question was called on the motion and it carried by unanimous vote.