Personal Identifying Information Subcommittee
of the FOIA Council
August 22, 2007 Meeting Summary

The Personal Identifying Information Subcommittee (PII Subcommittee) held its third meeting to discuss several bills referred to the FOIA Council for study by the 2007 General Assembly[1]. This meeting was also the second joint meeting with the JCOTS Social Security Number Subcommittee[2] to examine HB 2821 (Sickles), which would exempt from the mandatory disclosure requirements of FOIA those portions of records containing an individual's social security number.

The bulk of the meeting involved staff presentations to assist the Subcommittees in their deliberations and in response to requests for information made at the prior joint meeting. Specifically, staff reported on (i) other states' law concerning access to social security numbers (SSNs) for both the private and public sectors; (ii) federal law and trends on the subject; (iii) specific Virginia laws governing access/availability to SSNs, including the Personal Information Privacy Act (§ 59.1-442 et seq.), FOIA (§ 2.2-3700 et seq.), and the Government Data Collection and Dissemination Practices Act (§ 2.2-3800). A summary of each staff report follows. Copies of the staff reports are posted on the FOIA Council's website.

OTHER STATES' LAWS

Preliminary research reveals that many states have enacted laws that restrict access to SSNs in public records and in the private sector. The language and specifics of these laws differ from state to state. Some states' law applies only to the private sector and imposes restrictions on the collection and dissemination of SSNs in connection with commercial transactions. In examining the various means through which the acts restrict access to SSNs, however, there appear to be some common themes.

Many states, including Virginia, restrict the display of SSNs on government-issued identification cards and restrict the mailing of documents in which SSNs are visible either on the envelope or through a window on such envelop. Other states, in a commercial setting, prohibit requiring individuals to transmit SSNs over the Internet unless the connection is secure or the SSN is encrypted. According to research conducted by Gail Hillebrand, Financial Services Campaign Manager, Consumers Union, "...California enacted legislation in 2001 that generally prohibited businesses from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, mailing documents that display SSNs before the document is opened, printing SSNs on cards necessary for accessing products or services, or requiring people to transmit a SSN over the Internet..." According to Ms. Hillebrand's research, "[T]wenty one states have passed laws similar to California's--Arizona, Arkansas, Colorado, Connecticut, Georgia, Hawaii, Illinois, Maryland, Michigan, Minnesota, Missouri, New Jersey, New Mexico, New York, North Carolina, Oklahoma,

[1] Senator Houck, Delegate Griffith, and subcommittee members John Edwards, Mary Yancey Spencer, Sandra Treadway, and Courtney Malveaux were present. No members were absent.
[2] Delegates May and Alexander and Senator Watkins.

Pennsylvania, Rhode Island, Texas, Utah, and Virginia." It is important to note, however, that by its express terms, California law "does not apply to documents that are recorded or required to be open to the public" pursuant to law.[3]

Public Records Specifically

Research in this area was limited for the most part to those states that have had a separate FOIA ombudsman program in place since 2000-- namely New York, Connecticut, Minnesota, Hawaii, and Indiana. In addition, North Carolina and Florida were included based on unique provisions in their statutes restricting the collection and dissemination of SSNs in public records. Statutory trends among these states reveal differing approaches, although four general approaches emerge.

- Statutory presumptions that SSNs collected or maintained by a state agency, statewide system, or political subdivision are private data, except to the extent that access to SSN is specifically authorized by law. See § 13.355 of the Government Data Practices Act of Minnesota and § 119.071 of the Florida Public Records Act.

- Statutory prohibitions on agencies of the state or its political subdivisions, or any agent or employee of a government agency from doing any of the following: (i) collect a SSN unless authorized by law to do so or unless collection of a SSN is imperative for the performance of that agency's duties and such need is clearly documented; (ii) fail to segregate a SSN from the remainder of the public record; or (iii) intentionally communicate or otherwise make available to the general public a person's SSN or other identifying information. See § 132.1.10 of the North Carolina Public Records Act, § 4-1-8 of the Indiana Code, and § 119.071 of the Florida Public Records Act.

- A statutory exemption restricting release if it would constitute
    - (i) "An unwarranted invasion of personal privacy." See § 89 of the Freedom of Information Law of New York and § 96 of the Personal Privacy Protection Law of New York; or
    - (ii) "An invasion of personal privacy." See § 1-210 of the Freedom of Information Act of Connecticut.

- A statutory exemption restricting release of entire SSNs, with some exceptions; although release of last four digits only is permissible. See § 487J of the Social Security Number Protection Act of Hawaii and § 4-1-10-1 of the Indiana Code. NOTE: Hawaii law provides for civil penalties for violation by businesses and liability in equal amount to the sum of actual damages sustained by the injured party. Indiana law provides for criminal penalties in the event of violation by state agencies and for fraudulently obtaining a SSN from a state agency.

In conclusion

[3] See § 1798.85 of the California Civil Code (2007).

Preliminary research appears to show that most of the legislative activity relative to the release of SSN is found in laws governing the actions of the private sector. This may be due in large part because historically it is breaches in the private sector that have put individuals at heightened risk of identity theft. As noted above, however, several states have enacted laws to govern the release of SSNs found in public records and such laws appear to focus on limiting the collection of SSNs by governmental entities in the first instance, followed by a restriction on the release of an entire SSN as a matter of law or, as in New York and Connecticut, where release of the SSN would constitute an invasion of personal privacy.

FEDERAL LAW AND TRENDS

Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain (GAO-07-752, June 2007)

The federal government has recently examined the availability of social security numbers in public records. This June, 2007 Government Accountability Office report recommended, at a minimum, that social security numbers be truncated in liens and lien releases issued by the Internal Revenue Service, and that federal agencies should continue to take steps to mitigate the availability of social security numbers in public records.

Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16, May 22, 2007)

The United States Office of Management and Budget also recently issued a memo to the heads of all federal executive agencies and departments directing each agency to safeguard against the breach of personally identifiable information. The memo requires all agency and department heads to implement a framework for ensuring proper safeguards are in place to protect personal information collected by the agency, and to develop a breach notification policy.[4] Most notably, however, for purposes of discussion of this FOIA/JCOTS Subcommittee, is the directive to agencies to review their use of social security numbers and to identify when such use or inclusion of such information in a document or program is superfluous. Agencies were directed to eliminate the unnecessary collection and use of social security numbers within eighteen months (roughly the end of 2008). Agencies were also directed to participate in a government-wide effort to explore alternatives to the use of a social security number as a personal identifier.[5]

[4] JCOTS has previously discussed the issue of database breach notification as it relates to private entities, but recommended that federal legislation be adopted to address this issue to ensure uniformity of response to a breach. However, JCOTS work did not examine database breach notification as it might apply to information held by public bodies. Because the focus of HB 2821 and SB 819 is about public access to personal information, this memo will not delve into the database breach issue. However, substantial information about this topic could be made available, upon request.

[5] *Federal Initiatives*, prepared by Lisa Wallmeyer, Executive Director, JCOTS.

VIRGINIA LAW--*CURRENT RESTRICTIONS ON USE OF SOCIAL SECURITY NUMBERS*

A survey of Virginia law relative to the use of SSNs was conducted by staff and revealed that certain steps have been taken by the General Assembly to limit the dissemination of SSNs in both the private and public sectors. Much of Virginia law on this topic mirrors what has been done in other states. But like other states, Virginia's law has taken a piece meal approach rather than addressing these issues in a comprehensive, systematic manner. That is the goal of the Subcommittees' work. A summary of relevant Virginia law follows:

I. Government/Public Sector (excluding FOIA):

- Health Insurance ID Number for State Health Plan shall not be an individual's social security number (§ 2.2-2818 (N)).
- No agency can require an individual to supply his social security number or refuse services to an individual for refusal to supply his social security number, unless the disclosure is specifically required by state or federal law (§ 2.2-3808 (A)).
- No agency-issued ID cards (such as student identification cards and license certificates) may display an **entire** social security number -- all such existing cards were required to be replaced by July 1, 2006 (§ 2.2-3808 (B)).
- Voter registration cards displaying a social security number must all be reissued by December 31 following the completion of redistricting after the 2010 census (§ 2.2-3808 (C)).
- A clerk of court may refuse to accept any instrument submitted for recordation that includes a grantor's, grantee's, or trustee's social security number (§ 17.1-227).
- No clerk of court shall disclose a social security number, other identification number, or financial information provided to the clerk to pay fee, fines, taxes, or other charges (§ 17.1-293(A)).
- No clerk may post social security numbers or other specified identifying information on the Internet, except as provided in remote access subscription services (§ 17.1-293 (B)).
- The clerk of court may withhold from public disclosure a social security number provided on an application for a concealed handgun permit (§ 18.2-308(D)).
- Petitions, pleadings, motions, orders, etc. regarding divorce and child custody shall not contain the social security numbers of any party or of any minor child. If required by law, social security numbers shall be provided on a separate addendum that will not be made available to the public (§ 20-121.03).
- Election records containing social security numbers shall not be made available to the public (§ 24.2-107).
- Social security numbers shall only apply on applications for marriage licenses retained by the officer issuing the license, and on the copy of the license forwarded to the State Registrar. Marriage licenses that were filed after July 1,

1997 and that are not configured to prevent disclosure of a social security number shall not be available for public inspection (§ 32.1-267 (E), (F)).
- Social security numbers shall not be used as driver's license numbers (§ 46.2-342 (A)).

II. Private Sector:

- A consumer may request that a supplier not use the consumer's social security number as his account number (§ 59.1-200 (A)(35)).
- A person may not intentionally communicate an individual's social security number to the general public. However, this prohibition does not apply to public bodies or public records (§ 59.1-443.2 (A)(1), (D)).
- A person may not print an individual's social security number on any card required to access or receive products or services. (§ 59.1-443.2(A)(2)).
- A person may not require an individual to use his social security number to access an Internet website, unless a password or other authentication is also required (§ 59.1-443.2(A)(3)).
- A person may not send any letter or package that displays a social security number on its face or from which the social security number is visible (§ 59.1-443.2 (A)(4)).
- No person can embed a social security number (even if encrypted) in or on a document using a bar code, magnetic strip, or other technology, in place of removing a social security number as required by the Personal Information Privacy Act (§ 59.1-443.2 (E)).[6]

III. FOIA:

A review of FOIA and exemptions contained therein allowing the withholding/redaction of SSNs in particular and personal identifying information in general, revealed that such information is protected in 39 specific instances from release in records relating to, but not limited to, protection in the context of public employment, scholastic records, health records, rape crisis centers and programs for battered spouses, subscriber data provided to state and local government by telecommunication carriers for implementation of the E-911 emergency dispatch system, certain license and permit applications, involuntary admission proceedings, public assistance programs, child support enforcement, and child welfare, recipients of public housing assistance, recipients of TANF transportation services, state and local tax information, public library records, certain customer account information (public utilities and SmartTag, etc.), witnesses and victims of crime, neighborhood watch, citizen emergency response teams, and statewide alert network participants. A complete list of the protection of citizens' personal identifying information under FOIA is available on the FOIA Council website.

IV. Government Data Collection and Dissemination Practices Act (GDCDPA):

[6] *Current Restrictions on Use of Social Security Numbers in Virginia,* prepared by Lisa Wallmeyer, Executive Director, JCOTS.

Enacted in 1976 under the name of the Privacy Protection Act of 1976, the GDCDPA does not in actuality protect privacy. The Privacy Protection Act was renamed in 2003 to the GDCDPA because it is more akin to the Fair Credit Reporting Act in that it gives "data subjects" the right of access to government records of which they are the subject and the right to correct inaccurate information contained in those records. In 1976, the General Assembly made the following findings which are embodied in the GDCDPA:

> 1. An individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;
> 2. The increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;
> 3. An individual's opportunities to secure employment, insurance, credit, and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and
> 4. In order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

With the advent of the Internet, widespread use of computers, and the automated collection and storage of data, the principles expressed in the GDCDPA have been given renewed attention. It is important to note, however, that the GDCDPA has no provisions for enforcement.

STUDY PLAN OPTIONS AND CONSIDERATIONS

To assist the Subcommittees in achieving a systematic and comprehensive examination of the collection and dissemination of SSNs in Virginia, staff prepared relevant questions for the consideration and development of sound public policy relating to SSNs. The following outline will serve as a basis for the Subcommittees' work and to focus deliberations.

- **I.** Protection of SSN:
  - A. Why is protection needed?
    - Fraud--real or perceived?
    - To what extent are government records implicated?
    - Online access vs. practical obscurity; is one more dangerous than the other?
  - B. Other alternatives:
    - Protection of victims of abuse and other vulnerable persons;
    - Others attempting to protect their privacy (i.e. unpublished numbers)
    - Heightening penalties for existing crimes (SB 1282, 2007)
  - C. If protection of SSN deemed necessary/advisable--
    - Protect in whole or in part;
    - General exemption or context specific (i.e. FOIA model);
    - Advisability of "opt out" provisions;
    - Advisability of allowing access to certain persons based on showing of legitimate business or other interest?

- Limit collection by governmental entities of SSN:
  - ***Should*** this be addressed? (GDCPDA attempts it; FOIA Council preaches it--(i.e., collect only if required by law and essential to mission) (See AO-08-06)); and
  - ***How to*** address? (Legislation or executive order).
- Appropriateness of a separate law from FOIA dealing with collection and access to SSN:
  - Establish general rule about access to SSNs/unique identifiers--(include collection limitations on government?)
  - Exceptions to general rule--access rights to persons with "legitimate business or other interests" (i.e. private investigators, media representatives, mortgage brokers, and real estate title companies, etc).

- **II.** What is "personal information?" Should definition be revised since original definition crafted in 1976? Under the current GDCDPA, "personal information" means:

  *"…[*a]ll information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information." (See § 2.2-3801 of GDCDPA).

- **III. Government (public records) vs. private sector (Personal Information Privacy Act § 59.1-442)--**Should there be a distinction in protection of SSNs and other unique identifying numbers?

DISCUSSION AND PUBLIC COMMENT

The members of the Subcommittees discussed several issues pertinent to the collection and dissemination of SSNs. Delegate Griffith pointed out that SSNs are collected on election petitions that end up in the possession of political party personnel who are not public officials or employees; it was not clear whether the petitions retain the SSNs when so disseminated. Delegate May indicated that someone had posted a public record containing his sister's SSN on the Internet, and because it was from a public land record, that posting did not violate Virginia law. Delegate Griffith noted that the current language of § 59.1-442 would prohibit someone from disseminating his or her own SSN to the general public. A man does just that in advertising his commercial identity protection service on television and radio. Senator Houck stated that it does not seem right that § 59.1-442 does not apply

to public bodies and public records. Delegate Griffith suggested changing the relevant statutory language of § 59.1-442 to allow individuals to disseminate their own SSNs voluntarily; to exempt its application to court clerks, the DMV and other public officials and employees who need to use and disseminate SSNs to carry out their work; but to prevent others from disclosing SSNs to the general public through dissemination of public records. Delegate May pointed out there are good uses of SSNs, such as allowing credit agencies to easily maintain individuals' credit histories and thus providing quick and easy access to lines of credit. Senator Houck asked for public comment from access advocates on this topic.

Dick Hammerstrom of the Free Lance-Star asked whether the person who published Delegate May's sister's SSN online did so just to show that she could. Delegate May responded that that was the stated reason. Jennifer Perkins, of the Virginia Coalition for Open Government (VCOG), indicated that as a general rule VCOG was not opposed to restricting the dissemination of SSNs, but was concerned that the actual language used not be overly broad. Additionally, the discussion leads to the question of how one defines a "beneficial use" of SSNs. Tom Falat, Virginia Information Technologies Agency (VITA), pointed out that in addressing secure remote access to court records, one of the questions was why someone wanted access. This process contrasts with the FOIA process, because it has never been part of FOIA to ask why someone wants records. Megan Rhyne, speaking as a Virginia citizen, indicated her concern that saying "shall not" in regard to SSNs is a slippery slope that could lead to restrictions on access to other personal information that should be publicly available, such as contact information. Craig Merritt, on behalf of the Virginia Press Association (VPA), suggested that one reason public bodies and public records may have been excluded from § 59.1-442 was so that that statute would not set FOIA policy "through the back door." Nicole Bocra, a private investigator, indicated that she regularly uses SSNs in her investigations, and that SSN information is easily available online from court records. She also asked how a restriction on dissemination would be enforced. Staff indicated enforcement would be through an individual right of action. Fred Norman, representing Northrop Grumman, indicated that the actual cost to the Commonwealth and localities to remove SSNs from public records would be huge.

Through further discussion among the Subcommittees, there was a consensus that the definition of "personal information" found in § 2.2-3801 of the GDCDPA should be updated for current use, and that there is a need to address the sheer amount of personal information collected by government. Senators Houck and Watkins and Delegate May all expressed their agreement that government simply is collecting too much personal information, and that it would be better to limit collection in the first place rather than try to restrict subsequent dissemination. There was also consensus to look at the possibility of using a single, uniform set of data that could be collected, rather than having various agencies collect different amounts and types of data on the same individuals. Senator Houck suggested that it would be best to approach the protection of SSNs in both the public and private sectors through legislation outside of FOIA, because these topics are more general and concern more than just access to public records. In addition, such an approach would do no violence to FOIA principles where motive for the request is immaterial. Senator Watkins suggested that FOIA Council and JCOTS staff contact various agency staff to find out what type(s) of personal data agencies really need.

Senator Houck then asked whether anyone from the public would like to comment; there was no public comment in response. At this point, the joint meeting of the FOIA and JCOTS Subcommittees adjourned. The meeting then continued solely as a FOIA Subcommittee meeting to address two pieces of draft legislation, one concerning access to concealed handgun permits, the other addressing access to constituent correspondence (HB 3097 (Cole) and SB 1106 (Chichester)).

The draft bill concerning concealed handgun permits codifies the opinion of the Attorney General issued in April, 2007, by providing that the Department of State Police (DSP) shall withhold from public disclosure permittee information submitted to DSP for purposes of entry into the Virginia Criminal Information Network (VCIN). Delegate Griffith pointed out that in addition to collecting permit information from the circuit courts to enter into VCIN, DSP itself also issues permits directly to nonresidents.[7] The draft as written does not address how DSP is to treat information collected for the purpose of issuing permits to nonresidents. It was agreed by general consensus that the draft should be amended to clarify that records about nonresident permits issued by DSP should be open, just as records held by the clerks of court concerning resident permits are open. Mr. Merritt indicated this was the first time he had seen this draft and so he reserved the right to comment upon it until after giving it a more thorough review. There was no other public comment on this draft.

Next the Subcommittee considered a draft bill regarding access to constituent correspondence sent to members of local government. The Subcommittee had asked staff to prepare this draft at its last meeting after considering the identical bills HB 3097 (Cole) and SB 1106 (Chichester). After staff presented the draft, the Subcommittee discussed how public records "in the transaction of public business" are subject to disclosure under FOIA, but other records of a purely personal nature are not. Mr. Edwards pointed out, for example, that a personal invitation to dinner sent to a local supervisor or council member would not be considered a public record because it is not in the transaction of public business. By contrast, a letter attempting the sway the vote of the supervisor or council member on a matter before the board or council would be "in the transaction of public business" and subject to disclosure under FOIA. Acknowledging that General Assembly members do have a correspondence exemption while members of local governing bodies do not, it was pointed out that there are significant differences between the General Assembly and a local governing body. For example, Delegate Griffith pointed out that three or four members is often a majority on a local body, whereas one would have to assemble 40 or more members of the House of Delegates to have an equivalent voting block. David Gayle, representing Stafford County, provided the example of a constituent who wrote to his supervisor about tax issues and included information about the constituent's own income and personal budget, including personal expenses for the constituent's own medical care. Mr. Gayle also provided the example of correspondence sent to a supervisor that contained personal information about a minor student. He stated that it was those types of personal information for which protection was sought. Mr. Hammerstrom provided the actual

[7] Virginia residents may obtain concealed handgun permits from the circuit court of the county or city in which they reside. Nonresidents may obtain such permits directly from DSP.

example of an email message forwarded to School Board members stating that they should meet (without public notice) at a private individual's home on a Saturday morning to discuss budget issues. His concern was that any correspondence exemption might be used improperly or worded too broadly, such that it withheld access to correspondence that should be accessible to the public. Senator Houck observed that despite continued research and discussion, there was little agreement regarding this issue and no apparent consensus to move forward. Delegate Griffith moved to table the draft legislation; the motion carried without objection. Senator Houck then adjourned this meeting of the Subcommittee. The next Subcommittee meeting will be held after the September 10, 2007, meeting of the full FOIA Council, on a date to be determined.

#