Joint Meeting of the Personal Identifying Information (PII) Subcommittee
and the JCOTS SSN Subcommittee
Meeting Summary
October 6, 2008

The Personal Identifying Information Subcommittee (PII Subcommittee)[1] held its third meeting of 2008 to discuss several bills referred to the FOIA Council for study by the 2008 General Assembly. This meeting began as a joint meeting with the Joint Commission on Technology and Science (JCOTS) Social Security Number Subcommittee,[2] continuing work begun last year regarding the collection, use, and dissemination of social security numbers (SSNs). In addition, the Subcommittees were advised of recent court cases involving disclosure of SSNs. After the joint meeting of both subcommittees adjourned, the PII Subcommittee reconvened by itself to consider bills concerning access to concealed carry handgun permits.

Recent Court Cases

Council Staff advised the Subcommittees of recent court cases involving SSNs. The U.S. District Court for the Eastern District of Virginia heard the case of Chester Szymecki v. the City of Norfolk, involving the required furnishing of an individual's SSN. Procedurally, this opinion ruled on a motion to dismiss that argued that Mr. Szymecki's complaint alleged insufficient facts to state a claim upon which relief could be granted. On such a motion, the court must view the facts in the light most favorable to plaintiff. The relevant facts, so viewed and stated in brief, are that Mr. Szymecki and his family attended Harborfest, a public festival in Norfolk, Virginia. Mr. Szymecki was carrying openly a holstered handgun. A Norfolk ordinance prohibited such carry. Mr. Szymecki was detained and charged with violation of the ordinance. Mr. Szymecki stated that officers demanded his SSN, telling him he could either provide his SSN and be issued a summons, or be arrested and incarcerated if he refused. The police did not state why they needed his SSN, the authority for collecting it, or how it would be used. He provided his SSN, and was issued a summons. The charges for violating the local ordinance were later dropped. Mr. Szymecki further alleged that when he later went to pick up his personal property from the police, they again demanded his SSN, stating that they would not return his property if he did not provide his SSN. Again, the police did not state why they needed his SSN, the authority for collecting it, or how it would be used. Mr. Szymecki again provided his SSN. Among other claims, Mr. Szymecki alleged a federal Privacy Act Section 7 claim for the improper collection of SSNs.[3] The court first found that Section 7 confers a legal right on individuals, and violations may be enforced through an action under § 1983.[4] The court further found that Mr. Szymecki had alleged facts sufficient to state a claim for violation of

[1] Delegate Griffith, and subcommittee members Wiley, Malveaux, Spencer, Treadway, and Whitehurst were present; Senator Houck was absent.
[2] Delegate May and Senator Watkins were present. Delegates Nixon and Alexander were absent.
[3] 5 U.S.C. § 552a Note ("Section 7" refers to § 7 of Pub. L. No. 93-579, 88 Stat. 1909 (1974)).
[4] Apparently the federal circuit courts are split on these points, and there is no relevant precedent in the Fourth Circuit.

subsections (a) and (b) of Section 7.[5] It is staff's understanding that this matter is set for trial on December 16, 2008.

In another U.S. District Court case in the Eastern District of Virginia, Ostergren v. McDonnell, the Court considered the prohibition on dissemination of SSNs obtained from public records contained in the Personal Information Privacy Act (PIPA).[6] Ms. Ostergren advocates for the removal of SSNs from public records, especially court records that are published online. She publishes the Virginia Watchdog website to further those efforts. Among other content on the website, Ms. Ostergren republishes public records that contain SSNs in order to emphasize her advocacy and illustrate the problem. As of July 1, 2008, amendments to PIPA would prohibit such republication of public records containing SSNs. Violators may be subject to fines up to $2500 per violation, investigative demands, and injunctions. The court found that Ms. Ostergren has standing to seek an injunction, as she has alleged an injury-in-fact traceable to enforcement of PIPA that may be redressed by court, and that the case is ripe for decision. In its analysis the court reviewed prior Supreme Court decisions, each of which was decided narrowly on its own facts, and each of which was decided in favor of allowing the publication of public records lawfully obtained. The general legal principal to be derived from these prior decisions would be that the government cannot punish publication of truthful information lawfully obtained about a matter of public significance, but again the court emphasized that the Supreme Court had decided each case narrowly and left open the possibility that a different set of facts might lead to a different conclusion. The court observed that SSNs are generally entitled to privacy as personal identifiers that may be misused. However, the court found that based on the record that the General Assembly did not provide funding for the redaction by court clerks of SSNs from court records, protection of SSNs is not a state interest of the highest order. The court also found that this matter - the protection of SSNs - is a matter of public significance, and that Ms. Ostergren's speech is political in nature and entitled to protection under the First Amendment. The court decided that PIPA is unconstitutional as applied to Ms. Ostergren's website as it presently exists, but further briefing would be required "on the propriety and scope of an injunction other than with respect to Ostergren's website as it exists."[7] It is staff's understanding that the parties have submitted additional briefs and are awaiting the final order of the court.

SSN Survey Update

Staff advised the Subcommittees that the deadline for submission of the SSN surveys was October 1, 2008 and that the survey information was being compiled, the results of

---

[5] *Id.* (the relevant portions of Section 7 read as follows: "(a)(1) It shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because such individual's refusal to disclose his social security account number .... (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.")

[6] Code § 59.1-443.2.

[7] In full, the Court concluded "that Virginia Code §59.1-443.2 is unconstitutional as applied to Ostergren's website as it presently exists. However, given the significant public interest issues presented by the spreading of SSNs on the Internet, the Court will require further briefing on the propriety and scope of an injunction other than with respect to Ostergren's website as it exists."

which would be presented at the November meeting of the Subcommittees. Staff also suggested that the amendments to the Government Data Collection and Dissemination Practices Act (GDCDPA), which are not effective until July 1, 2009, be revisited to ensure that the law, once effective, is clear on its face. Staff noted that any suggested amendments would be clarifying and/or technical in nature.

REAL ID

D. B. Smit, Commissioner of the Virginia Department of Motor Vehicles (DMV) informed the Subcommittees of the impact of federal law on driver's licenses and national security. Mr. Smit noted that previously a Virginia driver's license was merely a permit to operate a motor vehicle on public roads. Now, however, following the September 11, 2001 attacks and heightened requirements for proof of legal presence, the nature of driver's licenses has changed. Driver's licenses are unique identifiers. Mr. Smit stated that both state and federal law have changed to improve the integrity and security of state-issued driver's licenses and the issuance of identification cards in the U.S generally. He advised that the REAL ID Act was passed by the U.S. Congress in 2005 with a delayed effective date of May 2008. In conjunction with this act, the U.S. Department of Homeland Security issued final regulations in January 2008. He noted that Virginia and several other states have been given until December 2009 to implement REAL ID. Mr. Smit indicated that no states have REAL ID in place now, and that nine states have stated that they will not comply with its provisions because compliance is not currently mandatory.[8] He explained the REAL ID establishes national, minimum standards for the issuance of driver's licenses and ID cards, which include (i) information and security features incorporated into each card; (ii) applicant's proof of identity and U.S. citizenship status, and verification of the documents the applicant submits as proof; and (iii) security standards for DMV employees who issue driver's licenses and ID cards.[9] Essentially, driver's licenses and ID cards under REAL ID are an approved credential to get on an airplane or to gain access to certain public buildings. It is all about verification of identity. The full text of Mr. Smit's prepared remarks are available on the Council's website under the PII Subcommittee heading.

Discussion among the members of the Subcommittees relating to Mr. Smit's presentation focused on public access to sensitive information that will be submitted by Virginia citizens to DMV to verify their identity. Noting that the federal Drivers Privacy Protection Act and § 46.2-208 of the Code of Virginia currently protects against the release of personal information on individual licensed drivers, Mr. Wiley stated that § 46.2-208 needs to be revisited to insure the adequacy of protection of all of the additional information DMV will possess after REAL ID goes into effect in Virginia. The Subcommittees directed staff to work with the Office of the Attorney General on this issue.

The only public comment received was from Mike Stollenwerk, representing the Fairfax County Privacy Council, who suggested that Virginia should join the nine other

[8] The nine states are Arizona, Idaho, Louisiana, Maine, Montana, New Hampshire, Oklahoma, South Carolina, and the State of Washington.

[9] Excerpted from prepared remarks of D.B. Smit, Commissioner of Virginia DMV to the PII Subcommittee on October 6, 2008.

states in refusing to comply with the REAL ID Act. He noted that one can still fly without REAL ID but will be subject to increased questioning and screening.

Review of SSN bills

The Subcommittees turned their attention to the four SSN bills introduced by Delegate Sickles during the 2008 Session. Delegate Griffith indicated that without objection, HBs 1087 and 1088 would not be recommended by the Subcommittees, as they are too limited in scope. It was the unanimous recommendation of the Subcommittees that HBs 1096 and 1102 continue to be the subject of their deliberations in the hopes that consensus may develop for one or the other approach offered by these two bills to protect SSNs. Public comment was asked for and Mike Stollenwerk advised that he favors both bills.

With regard to HB 1096, establishing a Protection of Social Security Numbers Act, the Subcommittees discussed what they perceived to be the real problem with the bill. Specifically the provision that allow the disclosure of the last four digits of a SSN to enumerated entities, but not to the general public. Ginger Stanley of VPA indicated that VPA, as one of the enumerated entities in the bill, did not want any greater rights than the public, and suggested that the last four digits of a SSN be given out to the public. Staff indicated that under the bill, the release of the last four digits was limited to verification of identity and not a release of an actual redacted record. The Subcommittees asked for public comment on this provision. Mike Stollenwerk of the Fairfax County Privacy Council indicated that the last four digits of a SSN are the best part of an SSN, and that his organization objected to making the four digits public. He stated that the last four digits of a SSN are used the Department of Defense as a "PIN" (personal identification number). Mr. Wiley suggested that this provision be rewritten to allow public access to the last four digits of a SSN, notwithstanding this new act or FOIA. Mr. Wiley indicated that the real issue is how to deal with legitimate needs to verify identification of an individual. He stated that any system that may be adopted will be misused and there are criminal penalties for such misuse. Delegate Griffith asked whether there might be any middle ground for HB 1096. Delegate May asked what the VPA and data aggregators such as Lexis Nexis do in states that restrict access to SSNs. Delegate May stated that for verification of identity, with access to the last four digits of a SSN, there is a one in 2000 chance that one would have the correct person. He suggested legislation that would allow the release of the last four digits, but not the entire SSN. Mr. Theron Keller, interested citizen, indicated that because SSN is viewed as a key item, even release of the last four digits could lead to identity theft.

There being no additional public comment or other business, the joint meeting of the Subcommittees was adjourned. The Subcommittees set Wednesday, November 12, 2008 in Richmond from 10:00 a.m. to 2:00 p.m. (if needed) as their next meeting date. It is anticipated that this will be the last meeting of the Subcommittees and the time allotted to the meeting reflects the amount of work still to do, including review of the SSN survey results and any legislative fixes necessitated thereby.

PII Subcommittee of the FOIA Council

The PII Subcommittee separately (without the JCOTS Subcommittee) considered SB 529 (Houck), concerning access to concealed carry handgun permits. Delegate Griffith asked whether there were any proposed amendments to SB 529. Delegate Griffith arrayed the options for the PII subcommittee. It could (i) recommend again SB 529 in its current form[10], (ii) amend SB 529 to allow access to the database maintained by the Department of State Police to gun groups, (iii) propose a new approach to this issue, or (iv) close access to these records at the local courthouses. Public comment was requested and Mike Stollenwerk, Fairfax County Privacy Council, told the PII Subcommittee that all access to this information should be shut down; the concept expressed in Delegate Nutter's HB 982 (2008). There was no additional public comment. The PII Subcommittee voted unanimously to adopt SB 529 in its current form because they felt it reflected the proper balance between privacy and public access.

#

[10] The 2008 legislative recommendation of the FOIA Council.