OFFICE OF ATTORNEY GENERAL
STATE OF OKLAHOMA

March 15, 2010

Oscar Jackson, Administrator
Office of Personnel Management
2101 N. Lincoln Blvd.
Oklahoma City, OK 73105

Dear Mr. Jackson:

This is to advise you regarding the recent open records request your office received asking for, among other things, the employee identification numbers of all state employees. I believe employee identification numbers may be kept confidential under the Open Records Act, 51 O.S.Supp.2009, § 24A.28(A)(5)(b). That statute reads in pertinent part as follows:

> A. The following information may be kept confidential:
>
> . . . .
>
> 5. Information technology of a public body or public official but only if the information specifically identifies:
>
> . . . .
>
> b. system configuration information[.]

I asked Joe Fleckinger at the Office of State Finance ("OSF") to explain how "system configuration information" as used in the provision above may relate to employee identification numbers. As you may know, OSF operates and maintains the state's CORE/PeopleSoft system and monitors all traffic coming into the state's IT network. According to OSF, hackers frequently attempt to penetrate the state's system, from both inside and outside the United States. OSF constantly battles to maintain the integrity of the state's systems and data.

Employee identification numbers were created so that each individual employee would have a unique identifier in the CORE/PeopleSoft system without using the employee's social security number. The CORE/PeopleSoft system associates that employee identification number with all information within the system that relates to that employee, including time sheets, tax information, banking information (for purposes of direct deposit), payroll deductions, and other personal information, including social security number. Additionally, the employee identification number is used by Active Directory for employees of OSF and agencies supported by OSF to log into their computers and the applications to which they have been granted access. Active Directory is designed to be the standard method for all state employees to log into OSF's applications.

Obtaining the employees' names and identification numbers could allow someone to penetrate the PeopleSoft system by writing a simple program to try combinations of numbers to go with the first four characters of the employees' last names. The same program could be used to run through the entire list of employee identification numbers and effectively disable everyone's accounts in PeopleSoft in a matter of minutes. Further, if the program were smart enough to remember where it left off, eventually it would get a match, enabling it to access employees' accounts and all the information they contain. Hence, like social security numbers, employee identification numbers are a crucial piece of information in potentially accessing confidential employee information in OSF's data systems.

Given Mr. Fleckinger's information, in my opinion employee identification numbers fall within the exceptions cited above in 51 O.S.Supp.2009, § 24A.28(A)(5)(b) as "system configuration information." You may therefore keep employee identification numbers confidential in responding to open records requests.

Sincerely,

TOM GRUBER
FIRST ASSISTANT ATTORNEY GENERAL

TG:seh