THE ATTORNEY GENERAL
OF TEXAS

JIM MATTOX
ATTORNEY GENERAL

December 21, 1990

Mr. Jerome H. Supple
President
Southwest Texas State University
San Marcos, Texas 78666-4615

Open Records Decision No. 581

Re: Availability under the
Open Records Act, article
6252-17a,   V.T.C.S.,   of
source codes and related
documentation designed to
limit access to computer-
stored records   (RQ-2081)

Dear Mr. Supple:

Southwest Texas State University [hereinafter, the
"university"] has received a request for the following
information:

> 1. Source code and documentation to   the
> DEC-10 SADBDO and DADBDO [sic] programs, and
>
> 2. Computer program documentation standards
> required to be used by ADP programmers for
> DEC-10 programming.

You ask whether the requested information is subject to
required public disclosure under the Texas Open Records Act,
article 6252-17a, V.T.C.S.

The DEC-10 is the university's mainframe computer. You
describe the requested information as follows:

> The SADBDO and DAABDO programs are computer
> programs that allow authorized university
> officials to obtain information from the
> student records portion of the university's
> administrative data base. This information
> is used to prepare [student records].   The
> information includes students' grades and
> other personally identifiable   information
> from students' academic records.   Southwest
> Texas State University owns the copyright to
> both   programs.   Both   contain   security
> measures designed   to limit   unauthorized
> access to this data.

> Southwest Texas State University developed the source code and documentation that accompany these programs. The source code and documentation contain information that might compromise security measures designed to limit unauthorized access to the data.

> . . . .

> Likewise, the second item requested-- computer program documentation standards required to be used by the university's programmers for DEC-10 programming [developed at Southwest Texas State University]-- contains descriptions of security measures designed to prevent unauthorized access to student records.

A discussion of the issues raised by this opinion request requires some definition of the terminology.[1] Computer systems are, of course, made up of hardware and software. The hardware consists of the machinery, and the software controls the operation of the machinery. Software consists of sets of instructions called programs. Programs are written in defined sets of symbols called languages. A "machine language" is a set of electronic impulses which directly controls the machinery. A "high-level language" is closer in form to English and permits a programmer to compose and understand a program without being directly concerned with the operation of the machinery. Examples of high-level languages are C, COBOL, and PASCAL. Programs written in high-level languages must be converted into machine language by means of a program called a compiler.

A "source code" is a program, as described above, written in a high-level language. A source code describes the entire logical process or set of instructions to the computer used by the programmer to achieve the task that the program is designed to accomplish. In performing operations on a data base, a program must be able to locate and under-stand information contained or encoded within that data base. Therefore, a programmer literate in the language in which the source code is written can learn not only about

---

1. Reference is made to the glossaries and discussions in Raysman & Brown, <u>Computer Law: Drafting and Negotiating Forms and Agreements</u> (1990) (originally published 1984); Schwartz, <u>Computer Law Forms Handbook</u> (1986); Soma, <u>Computer Technology and the Law</u> (1983).

the program that the source code describes, but also about the organization and encoding of the data base that the program is designed to access or manipulate. Such information about the data base makes it possible for a programmer to create new programs to manipulate the data base. Generally, it is impractical to attempt to modify a program without access to the source code.

"Documentation" consists of an English language text describing various aspects of a program, such as how the program was written and how it may be used and maintained. Such documentation may be used either as a guide for users of the program, as a guide for programmers maintaining the computer system, or as a guide for future programmers who wish to understand the logic used in writing the program that the documentation describes. The nature and extent of documentation may vary depending on the purpose for which it is prepared.

You advise that the computer documentation standards are a set of features that programs designed for use on the DEC-10 are required to contain, and that apply to other programs in addition to SADBDO and DAABDO.

It is clear that dissemination of source code and documentation information regarding a computer program compromises the security of both the program itself and of the underlying data base. Given the extensive networking between computers and the necessity of numerous access terminals for most computer systems, physical restraints to access to the hardware cannot compensate for the loss of security features built into the software.

You assert a number of grounds for exception from required public disclosure for the requested information. In addition, we have received briefs in support of the university's position from the University of Texas System and Texas A&M University System. All the briefs cite the discussion in Open Records Decision No. 401 (1983), and we think it necessary to resolve the threshold issue raised in that open records decision.

Open Records Decision No. 401 concerned a request for computer programs used by the public works department of the city of Dallas [hereinafter, the "city"]. The city's initial contention was that the programs were not "public information" within the meaning of section 3(a) of the Open Records Act. In this respect the city argued:

> The data which composes [sic] the actual
> computer programs are merely scientific
> notations which indicate how public

information, which is either held in storage
or keyed in by an operator at some future
date, is to be used together (through
overlays, searches, compilations, etc.) to
produce additional public information which
can be used readily by the City in carrying
out its public function. In other words, the
program directs the compilation of or search
for public information. Taken alone, it is a
mere 'formula' without independent public
significance, and therefore does not fall
within the parameters of the Open Records
Act.

In a brief submitted in support of the city's position,
the University of Texas System argued:

We do not believe that computer software
constitutes a 'record' within the meaning of
the Open Records Act. Computer software is a
tool; it is a procedure to be followed in
operating upon data and, once loaded into the
machine, defines a set of electrical connec-
tions necessary to operate upon the data in
the desired manner. The very name 'software'
was chosen by the computer industry to
emphasize that a computer program is only an
extension of the computer 'hardware.' Use of
the Open Records Act to force disclosure of
computer software would be equivalent to
using the Act to force a State agency to
disassemble an office typewriter and photo-
graph the component parts.

Open Records Decision No. 401, noting that "informa-
tion" is a comprehensive term and that the form of informa-
tion is not relevant to the applicability of the Open
Records Act, concluded that the requested programs were
"information" within the meaning of section 3(a) and pro-
ceeded to consider the applicability of various of the
exceptions to public disclosure enumerated in that section.
With respect to programs developed by the city, Open Records
Decision No. 401 stated:

To the extent that use of a program would
enable the user to gain access to a
government computer or its memory banks in an
unauthorized fashion, for example, the
program may be withheld.

Programs that give access to
computer-stored information are analogous, in

that respect, to the combinations of safes. Safe combinations are merely notations of mechanical adjustments that must be made to gain access to the contents of the safe. The security of the information can be very important, even vital, depending on the contents. The same is true of information allowing access to government computers. Just as there is a difference between (a) making public particular documents kept in a safe and (b) releasing the safe's combination, there is a difference between (a) making available information stored in a computer and (b) making available information about how to get into the computer. The Open Records Act does not require governmental bodies to disclose information that would breach the security of government computers or computer files any more than it requires them to disclose the combinations of safes that might be on their premises.

No statute specifically makes the combinations of government safes, or programs accessing government computers, confidential information. [Cite omitted.] Nevertheless, the duty to guard them from unauthorized access is implied by statutory provisions such as section 4.01, article 601b, V.T.C.S.

. . . .

Statutory responsibility for the proper care and protection of the property of the state from damage, intrusion or improper usage (1) implies a power to reasonably maintain the confidentiality of information if release of it could result in such damage, intrusion or improper usage and (2) satisfies the requirement that exceptions to the Open Records Act entitlement to information be "expressly provided by law."

In concluding that the requested computer programs were "information" within the meaning of section 3(a) of the Open Records Act, Open Records Decision No. 401 notes the comprehensive dictionary sense of the word "information," and we have no doubt that in the dictionary sense, "information" includes computer programs. However, in its broadest sense, "information" can include almost everything about the world that is capable of being perceived or imagined. A door key is a representation of "information" expressed as a pattern

of grooves or notches etched in an oblong metal blank. The sole significance of this information is its utility as a tool in matching the internal mechanism of a lock. One can place a door key on a photocopier and produce a graphic representation of that information. A skilled locksmith could then produce a duplicate key from the photocopied representation of the original. With respect to the re- quested information in question here, its sole significance is as a tool for the storage, manipulation, and security of other information.

It is axiomatic that the primary consideration in construing statutory language is the intent of the legisla- ture. Citizens Bank of Bryan v. First State Bank, Hearne, 580 S.W.2d 344, 348 (Tex. 1979). A statute should also be construed in a way which best carries out its manifest intent. Id. We further believe that it requires no cita- tion to note the legislature's awareness of the responsibil- ity of public officers and employees for public property entrusted to their care. Accordingly, we cannot believe that the legislature could have intended that the Open Records Act compromise the physical security of information management systems or other government property. Nor is such a result necessary to accomplish the often-quoted purpose set forth in the preamble to the Open Records Act to provide the people with "full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees." While Open Records Decision No. 401 suggested an implied exception with respect to the requested computer programs, we no longer believe it necessary to find an implied confidentiality for the programs, but simply to recognize that the legislature could not have intended that such tools be the kind of "information" comprehended by the term as used in section 3(a). The rationale of Open Records Decision No. 401 is overruled to the extent it is inconsistent with this opinion.

The term "information" as used in the Open Records Act is certainly comprehensive and this opinion in no way limits the applicability of the term only to records required to be kept by law or which can be demonstrated to have some public significance. Industrial Found. of the South v. Texas Indus. Accident Bd., 540 S.W.2d 668, 675-76 (Tex. 1976), cert. denied, 430 U.S. 931 (1977); see also 2 Braverman & Chetwynd, Information Law: Freedom of Information, Privacy, Open Meetings, Other Access Laws § 24-4.2 (1985). However, where information has no other significance than its use as a tool for the maintenance, manipulation, or protection of public property, we find that it is not the kind of information made public by section 3(a) of the Open Records Act.
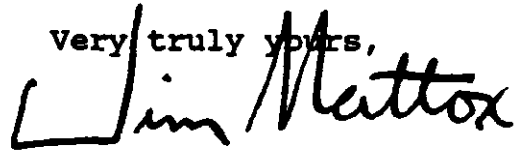
Of course, information maintained within computer information systems is subject to public disclosure unless excepted by the Open Records Act. However, the requestor in this case has not requested such information, and, at any rate, the information stored by the requested programs appears to be excepted in its entirety by sections 3(a)(14) and 14(e) of the Open Records Act.

As a result of this analysis, we need not examine the applicability of the various exceptions you raise. The requested information may be withheld.

S U M M A R Y

Where information has no significance other than its use as a tool for the maintenance, manipulation, or protection of public property, it is not the kind of information made public by section 3(a) of the Open Records Act. Accordingly, computer programs used by Southwest Texas State University to maintain records need not be released.

Very truly yours,

J I M   M A T T O X
Attorney General of Texas

MARY KELLER
First Assistant Attorney General

LOU MCCREARY
Executive Assistant Attorney General

JUDGE ZOLLIE STEAKLEY
Special Assistant Attorney General

RENEA HICKS
Special Assistant Attorney General

RICK GILPIN
Chairman, Opinion Committee

Prepared by John Steiner
Assistant Attorney General