



**THE ATTORNEY GENERAL
OF TEXAS**

**JIM MATTOX
ATTORNEY GENERAL**

September 17, 1990

Honorable Mike Driscoll
Harris County Attorney
1001 Preston
Suite 634
Houston, Texas 77002

Opinion No. JM-1224

Re: Whether information relating
to criminal cases is subject to
disclosure and related questions
(RQ-1482)

Dear Mr. Driscoll:

You ask nine questions regarding the operation of the Harris County computer system and the authority of a board created by the Harris County Commissioners Court to manage the system. The questions stem from disagreements over the control of and access to information stored in the computer. Before considering your questions, we will briefly review the factual information supplied by your office and others.

In October of 1977 the commissioners court created a county department called the Justice Information Management System (JIMS), evidently for the purpose of operating and maintaining the county's central computer system.¹ The duties of the department include, among other things, the programming of the central computer to meet the needs of those county offices with authorized access to the system, the training of county officials and employees in the use of the computer, and the assignment of passwords and transaction codes to control access to information stored in the computer. Some of these tasks are performed in conjunction with the county data processing department.

Your request for this opinion is prompted by the use of the county computer to collect and maintain information regarding pending and closed criminal cases. You inform us that the district clerk, the district attorney, the county sheriff, the county criminal courts, the county pre-trial

1. As we understand it, the central computer is the only electronic data processing resource available to most county offices.

services agency, the county adult probation department and juvenile probation department, justices of the peace, and county constables all store information concerning criminal cases in the computer. Though controls are programmed into the system by JIMS and the data processing department, information originally collected and entered into the computer by one agency may later be retrieved and updated by other agencies or be integrated with information collected by other agencies. These conditions have raised questions concerning the "custody" and control of criminal case information stored in the county computer.

The commissioners court appointed an executive board to oversee the operation of JIMS and the computer system. The board was specifically empowered to "establish and audit security codes" and to "authorize data elements to be entered and to whom they shall be distributed." The board's membership is composed of the administrative judge of the district courts trying criminal cases, the presiding judge of the county criminal courts at law, a judge of one of the family district courts, a judge of one of the juvenile district courts, a justice of the peace, the district attorney, the district clerk, the county sheriff, and a county constable.

In 1985 the JIMS executive board executed an agreement with the Texas Department of Public Safety (DPS) regarding access to the Texas Law Enforcement Telecommunications Systems (TLETS), a statewide clearinghouse for information collected and exchanged between law enforcement agencies throughout the state. The system, managed and operated by the DPS, provides local law enforcement agencies access to the resources of the National Crime Information Center, the National Law Enforcement Telecommunications System, the Texas Crime Information Center, the vehicle registration files of the Motor Vehicle Division of the Texas Department of Highways and Public Transportation, and the driver's license files of the DPS.

Among other things, the agreement between the JIMS board and the DPS requires JIMS to abide by all applicable state and federal laws, as well as any policies and procedures adopted by the administrators of the information systems that comprise the network. Though the agreement is silent on the matter, the JIMS board apparently interpreted the agreement to also impose on it the duty to ensure compliance by all users of the system. Violation of

applicable policies may result in an immediate suspension of service.²

Security breaches at the county level prompted the JIMS board to adopt security policies and procedures governing access to the computer system and retrieval of information collected in criminal proceedings. The board now requires all persons with access to the system to execute a form acknowledging that they understand the security policies and that violation of the policies and procedures may result in termination of their employment. The board also has instituted a policy of unilaterally terminating access to the computer system by persons, offices, or departments deemed in noncompliance with the security policies. In 1986, this policy was invoked against the office of the district clerk for its refusal to execute the security forms.

With these facts in mind, we now proceed to your first set of questions.

1. If the district clerk enters information contained in instruments, pleadings, orders, and documents in criminal cases in the county's computer to produce indices, registers and dockets, are such electronic/computer records public? Does such information constitute exempt criminal justice information?
2. Are such computer records part of the district clerk's 'official records'?

These questions relate to the status of information collected by the district clerk from court documents and transmitted to the county computer. The information the district clerk transfers to the computer includes basic data such as the defendant's name and date of birth, the name of his attorney, and other information reflecting progress of

2. We are informed that the DPS, in the exercise of its discretion, designated the Harris County central computer system as the sole link to the TLETS network in Harris County. All local law enforcement agencies in Harris County that receive TLETS, including those not affiliated with the county government, must obtain access to the system through the Harris County computer.

the defendant's case through the court system. The district clerk maintains the original documents from which the information was obtained, a microfilm or microfiche copy of the document, or both. With this information the district clerk creates a number of separate documents including indices, case summaries, case status reports, calendars, and other documents relating to pending or closed criminal cases.

You have informed us of a case filed with the Texas Court of Criminal Appeals that deals with issues similar to the ones you pose. It is styled Houston Chronicle Publishing Co. v. The Honorable Charles Hearn, District Judge, 263rd District Court, Harris County, Texas, No. 20,998-01 (filed Nov. 22, 1989). At issue was an order of the administrative judge of the district courts of Harris County that forbids the district clerk and county sheriff from disclosing the street addresses or telephone numbers of any defendant in any criminal case in the district courts until an attorney is hired or appointed to represent the defendant.

A newspaper publisher and a reporter contested the order. They attacked it as an infringement of their right of access to court files under the First Amendment to the United States Constitution and article I, sections 8, 10, and 13, of the Texas Constitution. They filed a motion before the Court of Criminal Appeals for leave to file application for writs of mandamus and prohibition.

The Court of Criminal Appeals denied the motion without written order on March 7, 1990. As a result of this ruling, the order of the district judge prohibiting the district clerk and sheriff from releasing the specified information remains in effect. It is inappropriate in an opinion of the attorney general to review or interpret the orders of the courts mandating that certain information be kept confidential. See, e.g., Open Records Decision No. 560 (1990). And in light of the possibility of further litigation on this matter, we will defer answering your questions as they relate to records in the custody of the district clerk until the matter is finally resolved. If, following resolution of this matter, you still require an opinion on the status of the records of the district clerk, please resubmit your questions at that time.

3. What criminal history information, if any, which is maintained or which may be accessed through the county's computer may be disclosed by the district clerk and other county officials?

We assume that by use of the term "criminal history information" you refer to information relating to criminal cases, the disclosure of which may be governed by state or federal law and regulations.

Federal law and regulations govern the dissemination of criminal history record information by agencies that collect, maintain, and exchange such information with support provided by the federal government for such purposes. See 42 U.S.C. § 3789g(c); 28 C.F.R. § 20.21(b). Criminal history record information is defined as

information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release.

28 C.F.R. § 20.3(b). The federal regulations are intended to protect individual privacy and to insure that criminal history information, wherever it appears, is collected, stored, and disseminated in a manner that insures its completeness, accuracy, and security. Id. § 20.1.

State and local agencies maintaining and disseminating criminal history information with federal assistance are subject to certain restrictions on dissemination set forth in the federal regulations. See id. §§ 20.20 - 20.25. These restrictions do not apply to criminal history information contained in court records of public judicial proceedings. Id. § 20.20(b)(3). Thus, federal regulations have no bearing on the disclosure of criminal history information in records of public judicial proceedings that are in the custody of the district clerk. There remains, however, the issue of the disclosure of information from court records under state law, an issue left unresolved by the Houston Chronicle v. Hearn case. For this reason, we are unable to answer your third question as it relates to the district clerk at this time. We can answer the question as it applies to other county and district offices.

The federal regulations described here affect two categories of criminal history information: (1) information collected, stored, and disseminated by state or local agencies, and (2) information obtained from any United States Department of Justice criminal history record information system.

The regulations affecting state and local operations do not purport to make any criminal history information confidential, but authorize the states and local governments to determine the purposes for which criminal history record information may be disseminated pursuant to state law, executive order, local ordinance, or a rule, decision, or order of a court. Id. § 20.21(c)(3). The regulations do not limit dissemination by a state or local agency of criminal history information that originates from the agency itself. See Open Records Decision No. 144 (1976). One regulation allows dissemination to "individuals and agencies for any purpose authorized by statute . . . as construed by appropriate state or local officials or agencies." Id. § 20.21(b)(2). These provisions require consultation of the Open Records Act, V.T.C.S. article 6252-17a, and interpretations of the act by the courts and this office.

The availability of information relating to arrests under section 3(a)(8) of the Open Records Act was determined in Houston Chronicle Publishing Co. v. City of Houston, 531 S.W.2d 177 (Tex. Civ. App. - Houston [14th Dist.] 1975), writ ref'd n.r.e. per curiam, 536 S.W.2d 559 (Tex. 1976), and summarized in Open Records Decision No. 127 (1976). The holding in that case prohibits the disclosure to the public of the chronological history of an individual's arrests and their disposition. 531 S.W.2d at 187-88.

The federal regulations referenced here also address the dissemination of criminal history information contained in any United States Department of Justice criminal history information system, including NCIC. See 28 C.F.R. §§ 20.30 - 20.38. Dissemination of criminal history information contained in any such system is authorized in four instances. See id. § 20.33. In addition, the subjects of criminal history information are allowed access to their own criminal histories. Id. § 20.34; see Open Records Decision No. 565 (1990). These regulations are not germane to the office of district clerk, since it does not have access to Department of Justice criminal history information systems. County offices that have access to such systems must, of course, abide by federal regulations and policies in order to receive assistance from the information systems. See 28 C.F.R. § 20.36.

Consequently, county officials are not required to disclose to the public criminal history information maintained on the Harris County computer system that is collected by a county or district office, even if acquired without the assistance of any Department of Justice criminal history information system. Information obtained from these

federal sources may be disseminated in accordance with federal regulations.

State law also addresses the collection and dissemination of criminal history information by criminal justice agencies. Chapter 60 of the Code of Criminal Procedure, articles 60.01 through 60.09, was enacted by the 71st Legislature and became effective on September 1, 1989. Acts 1989, 71st Leg., ch. 785, § 6.01 at 3548. It delegates to the Texas Department of Criminal Justice (TDCJ) the responsibility of establishing a data base for a centralized criminal history record information system. Code Crim. Proc. art. 60.02(a). The DPS is given the duty of maintaining a data base for a computerized criminal history information system that serves as a "record creation point" for criminal history information maintained by the state. Id. art. 60.02(b).

Under chapter 60, criminal justice agencies are expected to maintain and report to the TDCJ and the DPS specified information relating to criminal cases, with certain exceptions. See id. arts. 60.05, 60.06(a). Criminal justice agencies must also provide other criminal justice agencies with access to their own criminal history information systems. The duties imposed on criminal justice agencies by article 60.06 are also imposed on the clerks of the district and county courts. Id. art. 60.06(e).

Information on an individual collected by the TDCJ and the DPS from criminal justice agencies and stored in a central location that consists of

an identifiable description and notation of an arrest, detention, indictment, information, or other formal criminal charge and a disposition of the charge including sentencing, correctional supervision, and release . . . is not subject to public disclosure except as authorized by federal or state law or regulation.³

3. This language parallels the definition of "criminal history record information" found at title 28, section 20.3, of the Code of Federal Regulations and quoted in a preceding paragraph.

Id. art. 60.06(b). This limitation does not apply to a document of a criminal justice agency that is the source of information collected by the TDCJ. Id. art. 60.06(c). Similarly, an individual's criminal history record may not be disclosed to the public by either a criminal justice agency or the Criminal Justice Policy Council if the record is protected by state or federal law or regulation. Id. art. 60.03(b). Chapter 60 thus requires an examination of other state and federal laws governing disclosure of criminal history information. See generally Open Records Decision No. 565 (1990).

4. Who is the 'custodian' of all or portions of the records contained in the county's computer?

This question is prompted by general concerns over the control and "custody" of information stored in the county computer. The JIMS board, you advise, contends it is the custodian of all information housed in the county computer and is thereby authorized to determine who may have access to that information. You emphasize that the question of control is significant because computer programming allows a county office to manipulate information in the computer files of other offices simply by updating information in its own computerized records. The example you give is a notation in the records of a court that a defendant in a criminal case is released on personal recognizance. Once this information is entered into the court's or the district clerk's computer files, the computer system automatically updates the information in computer files created for the same case by other county offices (e.g., the county sheriff or district attorney). You acknowledge that this may be an efficient use of the county computer, but you believe that it improperly wrests control from the hands of county officers who may have a legal duty to retain control over such information.

You argue that county officers, designated the custodians of records of their respective offices by the Open Records Act, should retain control of information maintained by their offices, including information housed in the county computer. We agree with your conclusion, but note that the issue of control is resolved by recent legislation.

Prior to 1989, there was little law expressly governing the establishment or operation of a computerized recordkeeping system for the use of county or district officers. See, e.g., Code Crim. Proc. art. 2.26 (repealed

in 1989, provided that commissioners court could authorize, among other things, the electronic entry, storage, and retrieval of records which the Code of Criminal Procedure requires county officers to keep); Gov't Code §§ 51.801 - 51.807 (authorizing the electronic filing of certain documents in district and county courts, subject to rules and procedures adopted by the Supreme Court of Texas). Authority for the establishment of a computer system by a commissioners court is now expressly recognized in the Local Government Code.

Subtitle C of Title 6 of the Local Government Code was amended during the 71st Legislative Session and designated the Local Government Records Act. Acts 1989, 71st Leg., ch. 1248, at 4996. Section 205.002 of the Local Government Code, enacted as part of the Local Government Records Act, provides that "[a]ny local government record data may be stored electronically in addition to or instead of source documents in paper or other media," subject to the provisions of chapter 205 of the Local Government Code and rules adopted under it. This provision authorizes the storage of information on computer. Local Gov't Code § 205.001(1) (definition of "electronic storage"). "Local government record data" is defined simply as any information that comprises a local government record under law, regulation, rule of court, ordinance, or administrative procedure. Id. § 205.001(2). With exceptions not applicable here, "local government record data" is defined to mean

any document, paper, letter, book, map, photograph, sound or video recording, microfilm, magnetic tape, electronic medium, or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under the laws of the state, created or received by a local government or any of its officers or employees pursuant to law, including an ordinance, or in the transaction of public business. (Emphasis added.)

Id. § 201.003(8).

The term "local government" includes, among other entities, a county, "including all district and precinct offices of a county." Id. § 201.003(7). District and precinct offices such as the offices of district attorney,

district clerk, justice of the peace, and constable are classified as county offices for the purposes of the act.

The subject of control and custody of information collected by county officers and stored electronically in a computer is addressed by the Local Government Records Act. The act identifies three agents of county government -- the commissioners court, "records management officers," and "custodians" -- and prescribes in careful detail their duties regarding the management and preservation of county records. See id. §§ 203.001 - 203.003, 203.021 - 203.023.

The "records management officer" is either an elected county officer or a person, office, or position designated by the governing body to serve in that capacity. See id. §§ 201.003(14), 203.001, 203.025. The duties of the records management officer vary, depending on whether the particular county office or department is elective or nonelective, but in either case the officer is made chiefly responsible for the administration of a records management program and the protection and preservation of the records of county offices. See id. §§ 203.002, 203.023. The "custodian" of records is the appointed or elected public officer who under state constitution, state law, ordinance, or administrative policy is in charge of an office that creates or receives local government records. Id. § 201.003(2).

A significant feature of the Local Government Records Act is its allocation of authority to develop and implement a records management program -- i.e., the policies, methods, and procedures for the management and preservation of county records. See id. §§ 203.005, 203.026. It is this aspect of the act that settles the general question of control and custody of information stored by computer.

The commissioners court is responsible for establishing a records management program for nonelective county offices. See id. §§ 203.021, 203.026. Elected county officers are designated the "records management officers" for their respective offices and are delegated preeminent authority to develop and administer the records management program for their offices. In addition, elected county officers are chiefly responsible for adopting records control schedules, preparing electronic storage authorization requests and records destruction requests, and preserving and protecting certain records of their offices. Id. § 203.002.

The elected county officer is given discretion to adopt specific records management procedures and techniques, so long as they are consistent with regulations promulgated by

the State Library and Archives Commission. See id. §§ 201.003(1), 203.002, 203.005(b). The commission is required to adopt standards and issue regulations for the microfilming of local government records and the electronic storage of local government record data of permanent value.⁴ Id. §§ 204.004, 205.003. It has discretion to adopt standards for the electronic storage of records with a retention period of at least ten years. Id. § 205.003.

These provisions specifically address certain kinds of records and limit the discretion of elected county officers to adopt management procedures for those records. We believe elected county officers have complete discretion in adopting records management procedures for computerized records or information not covered by these provisions -- i.e., any computerized record or information that does not have a retention period prescribed by law or that has a retention period of less than ten years. If the State Library and Archives Commission elects not to adopt standards for the electronic storage of records with retention periods of ten years or longer, we think elected county officers would have authority to adopt reasonable standards for those records as well. Moreover, we think elected county officers have the implied authority to prescribe reasonable security and control measures for any information received by their offices and stored electronically, even those records covered by the commission's rules. Cf. Bullock v. Calvert, 480 S.W.2d 367 (Tex. 1972) (public officers have implied power to achieve power or object expressly granted); V.T.C.S. art. 6252-17a, § 5(a) (described below).

The Local Government Records Act anticipates that elected county officers will establish an independent records management program for their offices, but allows elected officers to delegate the administration of the program to the office established by the commissioners court for nonelective county offices. Id. § 203.005(g). Elected county officers may also delegate their responsibilities to the records management officer for nonelective offices in lieu of adopting an independent program. Id. Applied to Harris County, these provisions mean elected county officers

4. A "record of permanent value" is one for which the retention period issued by the commission (the time during which the record may not be destroyed) is given as permanent. Local Gov't Code § 201.003(10).

may delegate the performance of their duties under the Local Government Records Act to JIMS if it is designated the records management officer for nonelective offices in Harris County.

In the absence of such a delegation of authority by elected county officers, the role of the commissioners court in the management of the records of elected county officials is largely supportive. Id. § 203.003 (commissioners court shall "promote," "support," and "facilitate" the efficient and economical creation, maintenance, management, and preservation of the records of elective county offices).

The primacy of elected county officers over the control and preservation of the records of their offices is also acknowledged in the Open Records Act. Section 5 of that act was amended by the bill enacting the Local Government Records Act to designate an elected county officer the "officer for public records" of the office. V.T.C.S. art. 6252-17a, § 5(a). The officer for public records is responsible under section 5 for ensuring the accessibility, protection, and preservation of public records, including records stored on computer. See, e.g., Attorney General Opinion JM-672 (1987).

These provisions clearly establish that control of information created or received by elected county officers⁵ pursuant to law or in the transaction of public business remains with the elected officers even when the information is stored in a computer system that serves all county offices. These provisions do not depart from established law, but merely reflect principles that are firmly entrenched in the law of this state. See Familias Unidas v. Briscoe, 619 F.2d 391, 404 (5th Cir. 1980) (elected county officials in Texas hold "virtually absolute sway over the

5. By its terms, the Local Government Records Act designates elected "county" officers as records management officers for their respective offices, omitting any reference to elected district and precinct officers. As we noted earlier, however, district and precinct offices of a county are treated as part of a county under the act. Id. § 201.003(7). By extension, when the act speaks of elective "county" offices, the legislature presumably intended to address elective district and precinct offices as well, at least where these offices store information on a computer system shared with county offices.

particular tasks or areas of responsibility entrusted to [them] by state statute").

Where the duties of county officers are clearly delegated by statute, the commissioners court has no power to displace the authority of such officers by the creation of an agency to perform such duties. See Aldrich v. Dallas County, 167 S.W.2d 560 (Tex. Civ. App. - Dallas 1942, writ dism'd); Navarro County v. Tullos, 237 S.W. 982 (Tex. Civ. App. - Dallas 1922, writ ref'd); Attorney General Opinion JM-1074 (1989). The commissioners court may not, moreover, confer on an agent or other officer authority the court may itself not exercise. Jones v. Veltrmann, 171 S.W. 287 (Tex. Civ. App. - San Antonio 1914, writ ref'd). An elected county officer's assumption of the powers and duties conferred by the Local Government Records Act effectively bars the commissioners court or its agent from displacing the county officer from this position of responsibility. See, e.g., Attorney General Opinion JM-1074 (1989).

Accordingly, in answer to your fourth question we conclude that elected county officers in Harris County are charged by statute with the control, management, and preservation of information created or received by their offices pursuant to law or in the transaction of public business, including information that is stored in the Harris County computer system. V.T.C.S. art. 6252-17a; Local Gov't Code §§ 203.002, 203.005, 205.002. Neither the commissioners court nor the agency created by it to manage the county computer system may deprive elected county, district, and precinct officers of this authority. Elected county officers may delegate certain of these duties to the office created by the commissioners court to manage the records of nonelective county offices. Id. § 203.005(g).⁶

6. It should be noted that article 60.09 of the Code of Criminal Procedure authorizes the commissioners court to appoint a "local data advisory board" to assist and advise the court on matters relating to the collection and transfer of criminal history information at the county level. The membership of the board parallels the membership of JIMS. See Code Crim. Proc. art. 60.09(b). Because the greater burden of compliance with chapter 60 falls on those officers eligible for appointment to the advisory board, we do not believe the authority to appoint advisory boards under article 60.09 constitutes supervening authority to manage
(Footnote Continued)

5. What authority does the executive board of the Justice Information Management System (JIMS) or the commissioners court have to enforce any state and/or federal statutes relating to the improper dissemination of criminal justice information and to require other county departments and/or officials to adhere to security and privacy guidelines promulgated by the executive board and/or commissioners court?

This question presumably relates to the security policies adopted by the JIMS board described earlier in this opinion.

As the discussion of the preceding question made clear, the primary responsibility to manage and control information received by elective county offices is with elected county officers and, for nonelective offices, with the commissioners court. Likewise, we think the duty to observe and comply with relevant laws governing access and dissemination of criminal justice information rests with elected county officers for their respective offices and with the commissioners court for nonelective offices. We have located no authority, including chapter 60 of the Code of Criminal Procedure, that would generally designate the commissioners court as the agency responsible for the enforcement of state or federal laws governing access to criminal justice information stored in the county's computer system. It is not inconceivable, however, that the commissioners court could, with the cooperation of elected county officers, promulgate effective security policies that preserve the power of elected county officers to manage and control the information collected and generated by their offices.⁷

(Footnote Continued)

the computerized records of all county offices. It is therefore unnecessary to consider the effect of the possible appointment of the JIMS board as the local data advisory board under this provision.

7. You have identified an obvious solution to the dilemma facing the county -- i.e., the installation of separate computer systems for each county office. Alternatively, the county might consider creating a separate

(Footnote Continued)

6. What liability may the JIMS executive board incur if information which is contained in a computer system owned by Harris County and which is used jointly by the Harris County Sheriff, the Harris County District Clerk, the Adult Probation Department, the Harris County Data Processing Department, and JIMS and other county departments for the functions of said respective departments and offices and JIMS is disseminated contrary to the security and privacy guidelines promulgated by the executive board, the commissioners court and/or other state and federal agencies?

This question is not one that can properly be answered by this office. Its speculative and fact-bound nature makes it appropriate for your office to advise its clients upon the development of appropriate facts in particular cases. See Gov't Code § 45.201.

7. Does the JIMS executive board and/or commissioners court have the authority to execute an agreement with the Texas Department of Public Safety regarding access to the National Crime Information Center (NCIC) operated by the Federal Bureau of Investigation (FBI) and the Texas Crime Information Center (TCIC) operated by the Texas Department of Public Safety on behalf of Harris County and other local law enforcement agencies that have access to Harris County's computer?

This question relates to the agreement executed by the JIMS board with the DPS described at the fore of this

(Footnote Continued)

computer system solely for the purpose of receiving and distributing criminal history information and information from the TLETS and NCIC networks that is accessible only by the law enforcement agencies entitled to participate in the networks. The efficacy of a particular proposal, however, is a matter for the discretion of the commissioners court and is beyond the province of this office to decide.

opinion. Assuming the DPS acted within its authority in selecting the Harris County computer as the county's link with the TLETS system, we think the commissioners court had the implied authority to execute the agreement in question. See generally, 35 D. Brooks, County and Special District Law § 5.13 (Texas Practice 1989). We also think the JIMS board was authorized to execute the agreement on behalf of the commissioners court, assuming the board was appointed its agent for that purpose pursuant to section 262.001(a)(3) of the Local Government Code. See generally, Jackson-Foxworth Lumber Co. v. Hutchinson County, 88 S.W. 412 (Tex. Civ. App. 1905, no writ).

8. May the county enter into agreements with public and non-public users for dial-up, direct computer access to records contained in the county's computer without the consent of the 'custodian/s' of the original paper or microfilm/microfiche of said records?
9. If the answer to question 8 is yes, is the 'custodian' responsible and liable for fees which may be due for such services? Who is liable if the fees are not collected for access to and/or copies of such records?

These questions are in reference to a program authorized by the commissioners court under which private parties, typically law firms, are allowed direct access to the county computer. The firms are granted access to information maintained by the district clerk on civil and family law cases in the district courts. Access to criminal and juvenile case information is not authorized. The private users receive access essentially on a subscription basis, paying the county fees for the training of the users' employees, the assignment of sign-on codes, and the amount of time logged on the county system. The users supply their own equipment and dedicated telephone lines.

You note the apparent absence of law expressly authorizing the program you inquire about.⁸ In addition "dial-up"

8. Sections 51.801 through 51.807 of the Government Code authorize and govern the electronic filing of certain
(Footnote Continued)

systems are particularly vulnerable to entry and manipulation by computer hackers and require additional security controls. See Agranoff, Curb on Technology: Liability for Failure to Protect Computerized Data Against Unauthorized Access, 5 Santa Clara Computer & High Technology Law Journal at 263, 280-86 (1989).

We have previously determined that elected county, district, and precinct officers, rather than the commissioners court or the JIMS department, are given the duty to manage and control the information received and generated by their offices and stored on computer. In the absence of statutory authority, the commissioners court is not, in our opinion, authorized to grant members of the public access to the computerized records of elective county, district, or precinct offices.⁹ In light of our answer to your eighth question, it is unnecessary to answer your final question.

S U M M A R Y

Elected county, district, and precinct officers in Harris County are charged by statute with the control, management, and preservation of information created or received by their offices pursuant to law or in the transaction of public business, including information that is stored in the Harris County computer. V.T.C.S. art. 6252-17a; Local Gov't Code §§ 203.002, 203.005, 205.002. Neither the commissioners court nor an agency created by it to manage the county's computer system may deprive

(Footnote Continued)

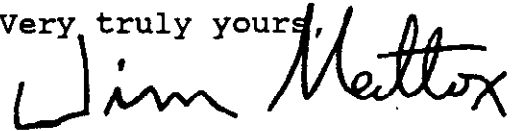
documents in the office of the district clerk, but we are unaware of any law that authorizes the electronic retrieval by private persons of information contained in documents filed with the district clerk.

9. You suggest that "dial-up" access to the records of county offices may be permissible if consent is given by the county officers whose records are affected and provided no confidential information is made available to the subscribers. It is unnecessary to decide this issue at this time, since your question refers to the "county" (which we interpret to mean the commissioners court) and the facts you stipulate refer to actions taken by the commissioners court rather than a specific county officer.

elected county, district, and precinct officers of such statutory authority. Elected county officers may delegate certain of these statutory duties to the office created by the commissioners court to manage the records of nonelective county offices. Local Gov't Code § 203.005(g).

Neither the commissioners court nor the agency created by it to manage the county computer system is generally authorized to enforce state or federal laws concerning the dissemination of criminal history information. The commissioners court has the implied authority to contract on behalf of the county with the Department of Public Safety to receive access to the Texas Law Enforcement Telecommunications System. The commissioners court may not authorize private users to obtain "dial-up" access to the records of elected county, district, or precinct officers that are stored on the county computer system.

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 Steve Aragon
Assistant Attorney General