STATE OF WISCONSIN
DEPARTMENT OF JUSTICE

J.B. VAN HOLLEN
ATTORNEY GENERAL

Raymond P. Taffora
Deputy Attorney General

114 East, State Capitol
P.O. Box 7857
Madison, WI 53707-7857
608/266-1221
TTY 1-800-947-3529

February 16, 2010 OAG-02-10

Mr. A. John Voelker
Director of State Courts
16 East, State Capitol
Madison, WI 53702

Dear Mr. Voelker:

¶ 1. You have requested my opinion regarding electronic transmission of certain confidential case information among clerks of circuit court, county sheriff's offices, and the Department of Justice ("DOJ") TIME System[1] through two new electronic interfaces involving the Wisconsin Department of Administration's Office of Justice Assistance ("OJA") Wisconsin Justice Information Sharing Program ("WIJIS") as a secondary transport system. In my opinion, applicable law permits these electronic transmissions through the new interfaces.

¶ 2. I understand that one of the new interfaces will transmit arrest warrant information to the county sheriff's office as an arrest warrant is issued by a circuit court using the Consolidated Court Automation Programs system ("CCAP"). The sheriff's office will add certain information, then transmit the warrant to the TIME System for purposes of notifying law enforcement statewide. When the warrant is executed, the sheriff's office will use the same interface to transmit service information back to the circuit court. In this opinion, I will refer to this as the "warrant interface."

¶ 3. The other new interface will perform the same functions for temporary restraining orders and injunctions issued pursuant to Wis. Stat. ch. 813. In this opinion, I will refer to this as the "protection order interface."

¶ 4. You indicate that the court system transmits other confidential case information through various electronic interfaces with other agencies, but that the warrant interface and the protection order interface differ in one critical aspect from those other interfaces. In addition to transmitting information through CCAP, the warrant interface and the protection order interface also utilize the secondary data transport system operated by WIJIS. Your questions arise because WIJIS does not have express statutory authority to independently obtain certain confidential data that would be transmitted through the warrant interface and the protection order interface.

[1]The Transaction Information for Management of Enforcement System, universally known as the TIME System, is a computer-based communications control center managed by the Crime Information Bureau at the Wisconsin Department of Justice. Its mission is to implement rapid and effective exchange of factual information between law enforcement agencies.

FACTUAL BACKGROUND

¶ 5. Understanding how the warrant and protection order interfaces work is necessary to frame my answers to your questions. CCAP Chief Information Officer Jean Bousquet ("Ms. Bousquet"), CCAP Customer Services Manager Andrea Olson ("Ms. Olson"), and WIJIS Program Manager Jeff Sartin ("Mr. Sartin") provided the following technical information, upon which my answers are based.

¶ 6. **CCAP Electronic Interfaces Generally**. According to Ms. Bousquet and Ms. Olson, CCAP's typical data exchanges with a justice system partner through an electronic interface start by establishing the data elements to be shared in incoming and outgoing messages: what information the courts will share electronically with the justice system partner, and what information the justice system partner will share with the courts. CCAP and the justice system partner then create a "schema" describing the structure of the electronic messages that will be used to exchange data. The schema is an organizational plan defining the data elements and attributes that can be included in an electronic message and providing for data verification. A data element is a particular category of information, like a person's surname. The attributes of a data element describe how the data element will be expressed in an electronic message, such as whether letters or numbers will be used. Extensible Markup Language ("XML") is used to structure the data elements and attributes in a specific electronic message, consistent with the plan established by the schema.

¶ 7. An electronic interface generally operates by transmitting XML electronic messages through CCAP's Simple Transport Exchange Protocol ("STEP") Server,[2] which is part of the court's secure wide area network. The STEP Server is an automated delivery service for electronic data exchanges; it accommodates the messaging services for all electronic data exchanges between the court system and its justice partners. A useful way to conceptualize the STEP Server is as a post office for electronic data messages.

¶ 8. An electronic data message transmitted through the STEP Server starts with preparation of the message at a sending agency by a computer program called a Publishing Client. The Publishing Client prepares the electronic data message in XML and then sends the message to the STEP Server. The Publishing Client creates and sends electronic data messages automatically when a triggering event occurs in the sending agency's database, such as issuance of a warrant by a judge. Message queues on the STEP Server hold and route messages for the various receiving agencies.

¶ 9. A receiving agency uses another computer program called a Subscribing Client to acquire the electronic data message from the STEP Server. After acquiring the message from the STEP Server, the Subscribing Client then updates the receiving agency's database with the information contained in the electronic data message.

---

[2]Ms. Bousquet indicates that the STEP Server actually consists of a cluster of servers performing messaging services for data transports. For clarity, this cluster of servers is referred to as the "STEP Server" in this opinion.

¶ 10. CCAP staff support and maintain the STEP Server hardware and its custom software. CCAP staff also troubleshoot transmission problems that arise as electronic data messages move through the data transport system. All CCAP staff and contractors are required to sign CCAP's Data Access Policy which, among other things, prohibits: (1) viewing any confidential or restricted information stored on any court system database for non-work purposes, or (2) discussing or disclosing any confidential or restricted information except as required for work.

¶ 11. **Electronic Interfaces for Arrest Warrants and Protection Orders**. The new warrant and protection order interfaces add another component to the typical information flow described above. In addition to routing the electronic data message through CCAP's STEP Server, it also is routed through WIJIS' workflow engine (the "WIJIS Workflow Engine"). One way to think of the WIJIS Workflow Engine is as an initial collection point for mail from law enforcement headed to the post office.

¶ 12. According to Mr. Sartin, the WIJIS Workflow Engine is a computer application housed on a dedicated server. The server is physically housed in DOJ's secure server area. Only a small number of WIJIS computer programmers are authorized to access the server that houses the WIJIS Workflow Engine, Mr. Sartin indicates, and must log in with passwords. These WIJIS personnel must pass the same stringent DOJ background checks as DOJ's computer services personnel.

¶ 13. Mr. Sartin indicates that the WIJIS Workflow Engine provides a uniform interface for the diverse records management systems used at various law enforcement agencies, and ensures that electronic data messages are sent securely. In the warrant and protection order interfaces, according to Ms. Bousquet, the electronic data message created by a law enforcement agency when a triggering event occurs is routed to the WIJIS Workflow Engine. The WIJIS Workflow Engine forwards the electronic data message to the message queue on CCAP's STEP Server for delivery to the court. Conversely, an electronic data message from a court to a law enforcement agency is transmitted to the STEP Server message queue. The WIJIS Workflow Engine retrieves the electronic data message from the STEP Server queue and then queues the message for pick up by the receiving law enforcement agency.

¶ 14. Ms. Olson advises that transmission of the actual warrant or protection order that triggered the electronic data message moving through an interface will vary by county. Some counties will scan the warrant or protection order and attach a scanned copy to the electronic data message moving through the interface. Other counties will continue to use existing physical transmission practices such as hand-carrying or faxing copies, which the receiving agency then will match up with the companion electronic data messages received through the interface.

¶ 15. As currently programmed, according to Ms. Olson, the XML electronic data messages that will travel through the warrant and protection order interfaces do not include an indicator that a particular document or the underlying action has been sealed. If the court orders the underlying action to be sealed after an electronic data message about a warrant or a protection order has been transmitted,

she advises, a second XML electronic data message would be sent to update the information transmitted in the first message; that second message would correct information in the receiving agency's database, not replace or erase the initial message.

¶ 16. The WIJIS Workflow Engine therefore operates like a mailbox, according to Mr. Sartin. A message is received, temporarily stored while queued on the secure system, then delivered to the authorized partner to which it is addressed. Because WIJIS processes data only for purposes of transmission, not for search or analysis, electronic data will be retained only temporarily on the WIJIS server for purposes of troubleshooting and delivery verification.

¶ 17. **Troubleshooting WIJIS Work Engine Problems**. Troubleshooting transmission problems that occur as electronic data messages move through the WIJIS Work Engine will be handled by WIJIS staff. In some cases, according to Mr. Sartin, that may involve opening and reviewing portions of a message to determine if the message has been corrupted or has other technical problems. Samples of the electronic data messages that will be transmitted through the warrant and protection order interfaces, provided by Ms. Olson, indicate that the messages are sufficiently comprehensible to be generally understood by a reader unfamiliar with the underlying legal action but knowledgeable about the applicable schema. WIJIS troubleshooting should not require opening the scanned warrant or protection order that might be attached to a particular XML electronic data message, according to Ms. Bousquet.

¶ 18. **Confidentiality Issues**. Your letter indicates that the vast majority of electronic data messages travelling through the warrant and protection order interfaces will not involve confidential information. Your inquiry instead is prompted by the relatively small number of warrants and protection orders involving legally confidential information.

¶ 19. Regarding the warrant interface, arrest warrants issued in juvenile cases are subject to the Wis. Stat. § 938.396(2) general rule of confidentiality for juvenile cases. Arrest warrants issued in criminal cases sometimes are ordered sealed; although rare, a criminal case itself may be ordered sealed. John Doe cases also may be sealed by court order pursuant to Wis. Stat. § 968.26. Between 2005 and 2008, your letter indicates, arrest warrants were issued in four criminal cases before those cases were sealed; no arrest warrants were issued in criminal cases after the underlying cases were sealed; and no arrest warrants were issued in John Doe cases that had been ordered sealed. With respect to some of your questions about the warrant interface, I also note that a small number of criminal cases are formally expunged from court records each year. *Cf.* Wis. Stat. § 973.015(2).

¶ 20. Regarding the protection order interface, you again indicate that orders to seal are not common. For the period 2005-2008, there was 1 order to seal domestic abuse protection order proceedings pursuant to Wis. Stat. § 813.12; 1 order to seal harassment protection order proceedings pursuant to Wis. Stat. § 813.125; and no orders to seal individual at risk protection order proceedings pursuant to Wis. Stat. § 813.123(3)(c). You note that orders to seal child abuse protection order

proceedings pursuant to Wis. Stat. § 813.122(3)(b) occur somewhat more frequently; during 2005-2008, orders to seal were issued in 30 of the 2,741 cases filed.

¶ 21. According to Ms. Olson, transmitting warrant and protection order information through the new interfaces is expected to be faster and more efficient than existing paper exchanges. Resulting database entries at the sending and receiving agencies also are expected to be more accurate because information no longer will need to be re-entered manually.

¶ 22. If the confidential information cannot be transmitted through the warrant and protection order interfaces, your letter indicates, that information will continue to be transmitted via paper copies. According to Ms. Olson, delivery mechanisms for paper copies currently vary by county but include facsimile transmission and personal delivery. Ms. Olson indicates that those existing mechanisms would continue to be used for confidential information if routing through the warrant and protection order interfaces is not legally permissible. Ms. Bousquet indicates that CCAP could connect directly to a small number of larger counties, but that incorporation of the WIJIS Workflow Engine also offers the benefits of electronic data transmission capacity to other smaller counties and provides a standardized law enforcement interface.

ANALYSIS

¶ 23. You ask a number of specific questions about transmission of information through the warrant and protection order interfaces. I have reorganized and restated your questions, as set forth below with my responsive answers.

¶ 24. All of my answers share two common premises, however.

¶ 25. First, an absolute right of examination applies to Wisconsin circuit court records required to be kept in the office of the clerk of circuit court. Wis. Stat. § 59.20(3);[3] *State ex rel. Bilder v. Delavan Tp.*, 112 Wis. 2d 539, 551-54, 334 N.W.2d 252 (1983).[4] The clerk must file and keep all papers properly deposited with him or her in every action or proceeding. Wis. Stat. § 59.40(2)(a); *Bilder*, 112 Wis. 2d at 554.

¶ 26. There are three exceptions to the "absolute right of examination" rule. First, documents may be closed to public inspection when a statute authorizes the sealing of otherwise public records. Second, documents may be closed to public inspection if disclosure would infringe on a constitutional right. Third, when required by the administration of justice, a circuit court may order documents or cases sealed pursuant to the court's inherent authority to preserve and protect the exercise of its judicial

[3]Wisconsin Stat. § 59.14 was renumbered as Wis. Stat. § 59.20(3) in 1995 Wisconsin Act 201, sec. 251. For clarity, the current statute number is used consistently in this opinion.

[4]Papers "required to be kept" are those that the custodian "is obliged by law to maintain or engender[.]" *State ex rel. Schultz v. Bruendl*, 168 Wis. 2d 101, 111, 483 N.W.2d 238 (Ct. App. 1992).

function. *Bilder*, 112 Wis. 2d at 554-56; *Madison v. Madison Human Serv. Comm'n*, 122 Wis. 2d 488, 491-92, 361 N.W.2d 734 (Ct. App. 1984) (statutory exception prohibiting disclosure of general relief applicants and recipients for purposes not connected with administration of relief programs). Your various questions implicate the first and third exceptions.

¶ 27. Second, the WIJIS Workflow Engine is just a conduit for electronic data messages passing through the warrant or protection order interfaces. Unless a transmission problem occurs at the WIJIS Workflow Engine, WIJIS staff have no need or reason to open any electronic data message, view the contents of any individual message, or generally browse the contents of messages passing through the interfaces. The troubleshooting role of WIJIS staff with respect to the interfaces therefore is the same as any other technician or contractor who might be called upon to deal with a problem in existing transmission mechanisms—such as fixing a malfunctioning FAX machine.

¶ 28. In an analogous situation, a particular non-confidential employee's technical ability to access sensitive collective bargaining documents stored on a public employer's computer was determined not to compromise the employer's proper expectation of confidence in collective bargaining matters. *Mineral Point Unified Sch. Dist. v. WERC*, 2002 WI App 48, ¶ 27, 251 Wis. 2d 325, 641 N.W.2d 701. Underlying that determination was the rationale that *de minimus* exposure to confidential information by a designated assistant in the proper course of official duties did not compromise confidentiality of the sensitive information. Lack of need, reason, or opportunity for support personnel to "browse" at will through confidential substantive information similarly characterizes the limited technical support role of WIJIS staff with respect to electronic data messages passing through the interfaces.

¶ 29. For any record-keeping system to function properly, information handlers such as technical consultants or clerical assistants must be able to see enough of the system to operate it properly. Information technology staff and contractors now function in logistical support roles previously occupied by secretaries and file clerks. Assuming other appropriate security measures, that limited technical access in the course of supporting official business is materially and permissibly different from impermissible, unrestrained access to confidential substantive information stored in restricted sections of CCAP's databases or other confidential court records.

1. *May electronic data messages about arrest warrants issued in juvenile cases that are confidential pursuant to Wis. Stat. § 938.396(2) be transmitted through the warrant interface?*

¶ 30. As your letter indicates, the Wisconsin Children's Code and Juvenile Code restrict access to court records of children and juveniles who are the subject of Wis. Stat. chs. 48 and 938 proceedings. Wis. Stat. §§ 48.396(2) and 938.396(2). Court records of Wis. Stat. ch. 938 proceedings "shall not be open to inspection or their contents disclosed except by order of the court assigned" or as allowed by

designated exceptions. Wis. Stat. § 938.396(2).[5] "Confidentiality is essential to the goal of rehabilitation, which is in turn the major purpose of the separate juvenile justice system." *State ex rel. Herget v. Circuit Court*, 84 Wis. 2d 435, 451, 267 N.W.2d 309 (1978). *See also* Wis. Stat. § 938.01(2).

¶ 31. CCAP therefore provides electronic information about these cases in restricted areas accessible only by authorized persons. Attorneys and others who would qualify under statutory exceptions to access information about some of these cases, but not others, cannot be allowed access to these restricted areas under existing provisions of Wis. Stat. §§ 48.396(2) and 938.396(2). The problem is that allowing such access would not prevent browsing—even inadvertently—through comprehensible information about confidential cases that a particular CCAP user was not entitled to access.

¶ 32. Conversely, authorized WIJIS technical personnel would not have unfettered substantive access to data moving through the warrant and protection order interfaces. Any such access, as described above, would occur only when required to troubleshoot electronic data transmissions necessary to effectuate court orders and facilitate court operations. WIJIS personnel who might incidentally see juvenile case information while troubleshooting a related electronic data message would not be browsing for substantive information. They instead would be functioning in a limited contractor-like technical capacity, essentially as court personnel, no different from a file clerk who makes photocopies of confidential court orders for mailing to counsel. Any incidental contact with confidential case information while serving the court is far different from opening a juvenile case file to the general public, and would further—by bringing the warrant subject into juvenile court—rather than undermine the rehabilitative purposes of the juvenile justice system.

¶ 33. Substantive content limitations cannot be applied to prevent necessary personnel from executing court functions. Juvenile case confidentiality restrictions, for example, must give way to other statutory provisions authorizing counsel to access court records of his or her clients. *State ex rel. S.M.O. v. Resheske*, 110 Wis. 2d 447, 329 N.W.2d 275 (Ct. App. 1982) (despite limited access provisions of Wis. Stat. § 48.396(2), it cannot be seriously argued that an attorney should not have access to a client's record in fashion not inconsistent with juvenile case confidentiality provisions).

¶ 34. Similarly, Wis. Stat. § 751.02 authorizes the supreme court to authorize employees it deems necessary for executing court system functions. *See also In re Janitor of Supreme Court*, 35 Wis. 410, 419 (1874) ("It is a power inherent in every court of record . . . to appoint such assistants; and the court itself is to judge of the necessity."); SCR 70.01(2)(a) and (d), 70.04 (responsibility and authority of the Director of State Courts for personnel and court information systems). Necessary personnel sometimes will be vendors or independent contractors, analogous to WIJIS' role with respect to the warrant and protection order interfaces. There is a difference between disclosing sealed or confidential records to the world at large, and disclosing them in an incidental, limited fashion to a

[5]In fact, Wis. Stat. § 48.981(7)(f) imposes strict criminal liability for unauthorized release of certain information related to information contained in reports and records made under Wis. Stat. § 48.981. *State v. Polashek*, 2002 WI 74, ¶ 35, 253 Wis. 2d 527, 646 N.W.2d 330.

professionally-interested and necessary person. *Cf. State v. Gilmore*, 201 Wis. 2d 820, 833, 549 N.W.2d 401 (1996). WIJIS technical personnel who might need to troubleshoot data transmissions along the warrant interface are professionally-interested persons necessary to sharing juvenile warrant information that effectuates operation of the juvenile courts.

¶ 35. The nature of any access by WIJIS technical personnel to juvenile warrant data transmissions travelling through the warrant interface therefore is qualitatively different from other impermissible access to confidential court records or information, such as allowing attorneys unrestricted access to CCAP areas containing confidential juvenile case information. In my opinion, this very limited access by WIJIS technical personnel would not violate Wis. Stat. § 938.396 confidentiality requirements.

2. *May electronic data messages about adult arrest warrants be transmitted through the warrant interface if either the warrant or the case in which it was issued has been ordered sealed by the court?*

¶ 36. The purpose of sealing an arrest warrant or a criminal case is to preserve secrecy and prevent disclosure to the public. *Cf. State v. Doe*, 2005 WI App 68, ¶ 11, 280 Wis. 2d 731, 697 N.W.2d 101. "[T]he more common meaning of disclosure involves making known or public that which has previously been held close or secret." *Gilmore*, 201 Wis. 2d at 833; *see also State v. Polashek*, 2002 WI 74, ¶ 19, 253 Wis. 2d 527, 646 N.W.2d 330. An arrest warrant might be sealed, for example, to prevent flight by the named person or to avoid alerting confederates of the named person.

¶ 37. In my opinion, sending transient electronic data messages about an adult arrest warrant through the warrant interface does not constitute making known or public the content of those data messages. The vast majority of messages will pass through the WIJIS Workflow Engine unopened and unviewed. To the extent that a specific transmission problem might require WIJIS' information technology personnel to examine a particular message in order to facilitate transmission of the message to its intended recipient, those information technology personnel are functioning only as professionally interested strangers with a very specific and limited role unrelated to substantive content of the message. Any incidental viewing of substantive content by WIJIS technical staff does not constitute making public the content of the electronic data message. The underlying purpose of sealing a particular warrant or case—to prevent disclosure to the public for an identifiable and significant reason—is not compromised by permitting WIJIS technical staff to troubleshoot transmission of the message. Access and disclosure restrictions imposed on WIJIS technical staff through a confidentiality agreement, as discussed in response to Question No. 7 below, would help insure that any WIJIS technical staff authorized to access messages flowing through the warrant interface understand and follow appropriate procedural parameters for opening and reading messages moving through the interface.

3. *May electronic data messages about an arrest warrant be transmitted through the warrant interface if the warrant was issued in John Doe proceedings that have been sealed pursuant to Wis. Stat. § 968.26?*

¶ 38. Yes, for the same reasons explained above in answer to Question Nos. 1 and 2.

¶ 39. I also note that secrecy may be an important aspect of a John Doe proceeding, of assistance to the fact-finding process, because:

> [i]t keeps information from a target who might consider fleeing; prevents a suspect from collecting perjured testimony for the trial; prevents those interested in thwarting the inquiry from tampering with testimony or secreting evidence; and renders witnesses more free in their disclosures.

State ex rel. Individual Subpoenaed v. Davis, 2005 WI 70, ¶ 20, 281 Wis. 2d 431, 697 N.W.2d 803 (footnote omitted). If a John Doe proceeding is secret, Wis. Stat. § 968.26 provides that "the record of the proceeding and the testimony taken shall not be open to inspection by anyone except the district attorney" unless and to the extent that it is used by the prosecution at preliminary examination or trial of the accused person. A proper secrecy order consequently covers questions asked, witnesses' answers, transcripts, exhibits, and other matters observed or heard at a secret John Doe proceeding. *Individual Subpoenaed*, 281 Wis. 2d 431, ¶ 21.

¶ 40. In my opinion, the reasons for keeping John Doe proceedings secret would not be compromised by allowing electronic data messages regarding sealed arrest warrants or sealed John Doe cases to travel through the warrant interface. Access to confidential substantive content would be strictly limited, as discussed above, and could be reinforced through an appropriate confidentiality agreement. Any such access would not amount to opening the matter for public inspection and would not threaten creating the premature disclosure problems that a John Doe proceeding is sealed to prevent. Moreover, electronic data messages travelling through the warrant interface would not include the types of information properly covered by a secrecy order: questions asked, witnesses' answers, transcripts, exhibits, and other matters observed or heard at a secret John Doe proceeding. The electronic data message instead would consist of a simple directive to arrest and produce a particular individual.

4. *May electronic data messages be transmitted through the protection order interface regarding a child abuse protection order in an action in which the court has ordered, pursuant to Wis. Stat. § 813.122(3)(b)3., that access to any record of the action be available only to the parties, their attorneys, any guardian ad litem, court personnel and any applicable appellate court? Similarly, may electronic data messages be transmitted through the protection order interface regarding an individual at risk protection order in an action in which the court has ordered, pursuant to Wis. Stat. § 813.123(3)(c)2., that access to any record of the case be available only to the*

individual at risk, parties, their attorneys, any guardian or guardian ad litem, court personnel and any applicable appellate court?

¶ 41. Yes, for the same reasons explained above in answer to Question Nos. 1 and 2. In this context, WIJIS technology staff function as an extension of the court personnel effectuating orders rendered by the court.

5. *May electronic data messages be transmitted through the protection order interface regarding a domestic abuse protection order issued pursuant to Wis. Stat. § 813.12 in an action which the court has ordered sealed? May electronic data messages be transmitted through the protection order interface regarding a harassment protection order issued pursuant to Wis. Stat. § 813.125 in an action which the court has ordered sealed?*

¶ 42. Yes, for the same reasons explained above in answer to Question Nos. 1, 2, and 4.

¶ 43. In addition, the domestic abuse protection order statute and the harassment protection order statute lack express provisions like Wis. Stat. §§ 813.122(3)(b)3. and 813.123(3)(c)2. that authorize a court to limit access to any record of the case. Both the domestic abuse protection order statute, in Wis. Stat. § 813.12(5m), and the harassment protection order statute, in Wis. Stat. § 813.125(5m) do provide that any petition or court order shall not disclose the address of the victim. Limiting the information contained in two specific documents does not amount to general sealing of the underlying action.

6. *For criminal, John Doe, or protection order cases that are sealed or expunged after issuance of a warrant or protection order about which an electronic data message has been transmitted through the warrant interface, should the court system require that WIJIS seal or expunge the case on the WIJIS Workflow Engine?*

¶ 44. Based on the technical information provided by Ms. Bousquet, Ms. Olson, and Mr. Sartin, it is my understanding that WIJIS will not retain any copy of a transient electronic data message passing through the warrant interface via the WIJIS Workflow Engine once delivery of the electronic data message has been verified. Therefore, nothing will remain at WIJIS to be sealed or expunged if a case is sealed or expunged after an arrest warrant is issued.

¶ 45. Furthermore, based on the same technical information, it is my understanding that correction of a previous electronic data message will be accomplished by sending another electronic data message to update the receiving agency's database—not by replacing or erasing the first message. Lack of any retained information at WIJIS accordingly distinguishes transfer of transient electronic information through the WIJIS Workflow Engine from CCAP's other data-sharing arrangements with justice partners who retain case information received from CCAP in the partners' own databases to be updated or expunged as subsequent events might dictate.

7. *Should CCAP enter into written agreements with WIJIS governing access by WIJIS personnel to case information contained in electronic data messages transmitted through the warrant and protection order interfaces. If so, what kind of provisions should these agreements include?*

¶ 46. Although not legally required, it would be a good business practice to execute written agreements with WIJIS clarifying and memorializing the limited purposes for which WIJIS personnel would be permitted to access case information in the electronic data messages transmitted through the warrant and protection order interfaces. Although the information that has been the primary subject of this opinion is confidential by law or court order, many other warrants and protection orders also implicate serious confidentiality concerns. Moreover, it is my understanding that the electronic data messages themselves would not indicate whether they involved a sealed warrant, sealed case, or other sealed matter. While a written agreement between CCAP and WIJIS regarding legally confidential or sealed information travelling through each interface would be beneficial, therefore, I also recommend that the access, use, and, disclosure provisions of those agreements apply to all case information moving through the interfaces regardless of whether it derives from a sealed or otherwise legally confidential matter.

¶ 47. Provisions similar to the CCAP Data Access Policy dated April 23, 2008, tailored to the nature of the information to which WIJIS personnel will have access and the reasons why WIJIS personnel may need to open electronic data messages for troubleshooting purposes, would be appropriate. Any confidentiality agreement also should specify the WIJIS personnel, by job classification or similar identification, who will be permitted to open and examine electronic data messages moving through the interface; how supervisory oversight of those personnel will be accomplished; and the availability of sanctions or discipline for violation of applicable confidentiality policies.

¶ 48. I hope you find this information helpful as these beneficial new criminal justice interfaces are finalized.

Sincerely,

J.B. VAN HOLLEN
Attorney General

JBVH:MEB:ajw:lkw