CALIFORNIA *SAMPLE*
Computer Search Warrant Language
(Where Digital Evidence Could be Present)

This resource is designed to be added to an existing search warrant format to enable an investigator to search for digital evidence and to remove digital evidence storage devices for off-site examination.

We are assuming that the affiant officer has already propounded appropriate language/facts within the warrant denoting that any desired digital evidence is either:

a) An instrumentality of the crime investigated; or
b) A storage container for illegal "contraband," such as child pornography; or
c) A storage container for evidence relating to the crime, such as "records."

Section 1 provides language for when the computer or other container containing digital media will be removed from the scene for search. Seeking removal of a computer used in a business environment for off-scene search should be discussed in advance with a prosecutor.

SECTION 1: Digital media is instrumentality of the crime and/or contraband or a container for evidence relating to the crime and will be removed for off-scene search.

A. The following is presented within the property section of the warrant.

FOR THE FOLLOWING PROPERTY:

1. Language Expanding The Definition of Property
Follows description of specific records to be searched for and seized

The terms "records," "information," or "property" includes all of the foregoing items of evidence in whatever form and by whatever means that may have been created or stored, including records, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic address books," calculators, or any other storage media, or any other form of "writing" as defined by Evidence Code section 250, together with indicia of use, ownership, possession, or control of such "records," "information," and "property."

Practice note: With the advance in technology, traditional paper records are now being increasingly discovered stored on computers and personal data assistants. Currently, the courts have been inclined to treat computers and other electronic storage devices as ordinary containers. Thus, warrants describing specified information are generally held to permit searches of containers capable of storing that

information. (See *New York v. Loorie* (1995) 630 N.Y.S.2d 483 (finding police did not exceed scope of warrant by searching contents of computer's internal drive and external disks when warrant only authorized taking possession of property).) However, since this issue has not been directly addressed by any California court, an affiant officer may still wish to include the following language describing how traditional paper records may now be stored.

2. <u>Language for Removing Computers for Off-scene Search</u>
Follows definition of property

Investigating officers are authorized, at their discretion, to seize all "computer systems," "computer program or software," and "supporting documentation" as defined by Penal Code section 502, subdivision (b), including any supporting hardware, software, or documentation that is necessary to the use of the system or is necessary to recover digital evidence from the system and any associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the seized items for the evidence described. Investigating officers and those agents acting under the direction of the investigating officers are authorized to access all computer data to determine if the data contains "property," "records," and "information" as described above. If necessary, investigating officers are authorized to employ the use of outside experts, acting under the direction of the investigating officers, to access and preserve computer data. Any digital evidence found during the execution of this search warrant will be seized, transported from the scene, and analyzed in a reasonably prudent time [**or you may want to consider the following**: *The investigating officer has* ***<u>(insert current forensic turn around time + 10 days)</u>*** *days from the date of seizure to determine if the seized computer systems and associated peripherals contain some or all of the evidence described in the warrant. Should additional time be required, the affiant shall show cause why more time is required and apply to the court for an extension.*] If no evidence of criminal activity is discovered relating to the seized computer systems and associated peripherals, the system will be returned promptly.

Practice note: When confronted with a computer at a search scene, searching officers have one of two choices; either search the computer at the scene or justify its removal in the search warrant for a subsequent search off-scene. The above language in conjunction with section B is suggested to justify removing computers for a subsequent search off-scene. (See *United States v. Kufrovich* (1997) 997 F. Supp. 246 [upholding warrant language authorizing removal of computer for latter search]; *United States v. Gawrysiak* (1997) 972 F.Supp. 853.) Note that the last three sentences state that the forensic examination will be completed within a specified time period. This is in response to a recent federal magistrate's ruling specifying short turnaround times of forensic examinations. (See *U.S. v. Brunnette* (D. Me. 1999) 76 F.Supp.2d 30 [suppression granted when investigator failed to comply with court-ordered forensic completion date]. The time period specified will reflect the current forensic completion cycle at the issuing agency, plus 10 days.

B. The following is presented within affidavit in support of the search warrant.

Note: *Language presenting facts that digital evidence is instrumentality and/or contains contraband or could contain evidence that is being sought and should be seized must be placed within the warrant.*

1. Affiant interviewed ***(insert law enforcement expert's name)*** employed as a ***(agent / computer examiner)***. Based upon information related to me on _____, I know that digital evidence can be stored on a variety of systems and storage devices including, but not limited to, electronic data processing and storage devices, computers and computer systems including central processing units: internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drive and tapes, optical storage devices or other memory storage devices: peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as modems.

2. ***(insert law enforcement expert's name)*** informed affiant that in connection with his employment, he uses computer systems as well as conducting computer-related investigations. In the past two years, ***(insert law enforcement expert's name)*** has supervised or participated in ***(insert number)*** executions of search warrants for computer-stored records and evidence. ***(insert law enforcement expert's name)*** informed affiant that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place, which could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without expert technical assistance. Since computer evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the entire period of the search.

3. **(*insert law enforcement expert's name*)** also stated that whether records are stored on floppy disks or on a hard drive, even when they purportedly have been erased or deleted, they may still be retrievable. **(*insert law enforcement expert's name*)** is familiar with the methods of restoring "lost" data commonly employed by computer users, and has used those methods himself. **(*insert law enforcement expert's name*)** has also obtained the assistance of a computer expert in several cases, in order to obtain the contents of computer-stored evidence where normal methods were unsuccessful. He stated that should such data retrieval be necessary, it is time-consuming, and would add to the difficulty of securing the system on the premises during the search.

4. **(*insert law enforcement expert's name*)** stated that the accompanying software must also be seized, since it would be impossible without examination to determine that it is standard, commercially available software: it is necessary to have the software used to create data files and records in order to read the files and records. In addition, without examination, it is impossible to determine that the diskette purporting to contain a standard commercially available software program has not been used to store records instead.

5. **(*insert law enforcement expert's name*)** informed affiant that the system documentation, instruction manuals, and software manuals are also necessary to properly operate that specific system in order to accurately obtain and copy the records authorized to be seized.

6. **(*insert law enforcement expert's name*)** informed affiant that the systems passwords or keys must also be seized, since it may be impossible to access the system if it is password-protected or other encryption devices are in place. **(*insert law enforcement expert's name*)** informed affiant that users often record passwords or keys on material found near the computer system. These passwords or keys could be names or a combination of characters or symbols.

7. **(*insert law enforcement expert's name*)** informed affiant that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies for a standard computer can take over 3 business days. Complex systems or recover tasks can require an excess of 45 business days to complete.

8. **[Insert only if requesting that the examination will be completed by a specified date]** *Due to the backload of computers awaiting to be examined and the limited number of trained examiners **(insert law enforcement expert's name)** informed affiant that **(examining agency)** is currently conducting searches of computer system within **(insert current forensic turnaround time)** days of receipt. **(insert law enforcement expert's name)** informed affiant that they would process any computer system seized pursuant to this warrant*

*within **(insert current forensic turnaround time + 10 days)** days of receipt.*

9. It is respectfully requested that I be allowed to seize all original digital evidence, in whatever form it currently resides, and transport this original digital evidence to a secure Evidence Storage Facility for a proper forensic examination.

Discovering Evidence Not Listed In Warrant During Search of a Computer
If records which are not authorized to be seized, or which relate to crimes not under investigation, are discovered in the course of analysis, the searching officer must obtain supplemental warrant to expand the scope of the original search warrant. (See *U.S. v. Grey* (1999) 78 F.Supp.2d 524.) While there is a argument that such records were lawfully discovered in "plain view," in light of current case law it is prudent that when the records are first discovered that the search warrant be expanded to encompass them.