JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

SPR22-27

Title
Rules: Remote Access to Criminal Electronic Records

Action Requested
Review and submit comments by May 20, 2022

Proposed Rules, Forms, Standards, or Statutes
Amend Cal. Rules of Court, rule 2.519

Proposed Effective Date
January 1, 2023

Proposed by
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

Contact
Andrea L. Jaramillo, 916-263-0991,
andrea.jaramillo@jud.ca.gov

Executive Summary and Origin

The Information Technology Advisory Committee (ITAC) proposes the Judicial Council amend rule 2.519 of the California Rules of Court[1] to authorize trial courts to provide private criminal defense attorneys broader remote access to criminal electronic records. The proposal originates with the California Attorneys for Criminal Justice, an advocacy organization comprised of criminal defense lawyers and associated professionals.

Background

The Judicial Council built "practical obscurity" into the rules governing access to electronic records by prohibiting public remote access to certain types of electronic records, including criminal electronic records, and limiting the viewing of such records to the courthouse.[2] This was intentional to help prevent widespread public dissemination of such records, which can contain highly sensitive personal information.[3]

[1] All further references to rules are to the California Rules of Court unless otherwise noted.

[2] Administrative Office of the Courts Manager Charlene Hammitt and Special Consultant Victor Rowley, mem. to Chief Justice Ronald M. George and Members of the Judicial Council, Dec. 10, 2001, pp. 1–6 (discussing the reasons for precluding remote access to specific electronic records in proposed rule 2073(c), the predecessor to current rule 2.503(c)). A copy of the memorandum is attached at pages 8–23.

[3] *Ibid.*

However, the Judicial Council recognized that there are persons and entities that are not the public at large, such as parties and their counsel, that the rules did not address and that courts were addressing in a piecemeal, ad hoc fashion.[4] Accordingly, nine Judicial Council advisory committees formed a subcommittee that developed rules for remote access to electronic records that is different than public access.[5] Under the remote access rules, criminal electronic records are available to specified users, including district attorneys, public defenders, and private criminal defense attorneys, but private attorneys are currently limited to remotely accessing their clients' records.[6]

The Proposal

The proposal would amend rule 2.519 to authorize the court to allow an attorney representing a party in a criminal action to remotely access any criminal electronic records the attorney would be legally entitled to view at the courthouse.

The purpose of the proposal is to ensure the rules on remote access treat private criminal defense counsel on par with public defenders and prosecutors. According to California Attorneys for Criminal Justice (CACJ), this change is needed because the current rules do not provide parity between private defense counsel and public defenders. For example, the current rules do not allow a private attorney to remotely access criminal electronic records other than those of their clients; thus, they could not remotely access electronic records in cases of witnesses or codefendants.

CACJ proposed amending rule 2.540 to include private counsel within its scope. However, rule 2.540 specifically addresses remote access by persons working for government entities only and is located in an article of the rules exclusive to government entities. As such, ITAC determined the proposed changes would be more suitable in amendments to rule 2.519, which includes private attorneys within its scope. Accordingly, ITAC developed a revised proposal to amend rule 2.519 instead of rule 2.540.

The proposed amendments authorize courts to allow attorneys representing a party in a criminal case to remotely access any criminal electronic records that the attorney would be entitled to view at the courthouse. The terms for remote access will apply in this instance. Specifically, the attorney:

- May remotely access the electronic records only for the purpose of assisting a party with that party's court matter.

---

[4] Judicial Council of Cal., Advisory Com. Rep., *Rules and Forms: Remote Access to Electronic Records* (Aug. 31, 2018), *https://jcc.legistar.com/View.ashx?M=F&ID=6613671&GUID=DA39F21F-B0F6-464E-8E33-1A771C41B679*.

[5] *Ibid.*

[6] Rule 2.519(a) & (b); rule 2.540(b)(1)(C) & (D).

- May not distribute for sale any electronic records obtained remotely under the rules in this article. Such sale is strictly prohibited.

- Must comply with any other terms of remote access required by the court.[7]

Failure to comply with these terms can result in sanctions, including termination of remote access.[8] These terms should help guard against the use of remote access for purposes such as selling access to electronic criminal records. The rule does not exclude additional consequences beyond termination of remote access for failure to comply with the terms of remote access. However, ITAC seeks specific comments on whether the rule should expressly identify additional potential consequences to convey the gravity of a violation more strongly.

In addition to the terms for remote access, the rules include other provisions designed to protect against unauthorized remote access or improper use of remote access. For example, rule 2.523 requires user identity verification, rule 2.524 requires remote access to sealed or confidential records to be "provided through a secure platform and any electronic transmission of the information must be encrypted," rule 5.525 limits searches to searches by case number or case caption, and rule 5.526 encourages courts to utilize audit trails so when an electronic record is accessed remotely, there is a record of that remote access.

Alternatives Considered

As discussed above, ITAC considered CACJ's proposal to amend rule 2.540, but determined that revising the proposal to amend rule 2.519 instead was more appropriate. Additional alternatives considered were the status quo, limiting remote access by public defenders rather than broadening remote access by private attorneys, and providing attorneys remote access to any electronic record they could access at the courthouse.

The Status Quo

ITAC considered taking no action. The problem with the status quo raised by CACJ is that a private attorney would still need to visit a courthouse to access certain criminal court records, for example, criminal court records of a codefendant, whereas a public defender or prosecutor would not. This is a concern if it may impact the quality of representation of a criminal defendant if needed records are burdensome to obtain. ITAC seeks specific comments on that issue.

The benefit of the status quo is that it limits the dissemination of criminal electronic records. Broadening remote access to criminal electronic records by private counsel would lessen the "practical obscurity" of such records. However, given that the proposed amendment is limited in scope as it applies only to attorneys representing parties in criminal cases, attorneys are bound by

[7] Rule 2.519(d)(1)–(3).

[8] Rule 2.519(d)(4).

professional obligations to be honest with the court,[9] and attorneys are bound by the terms of remote access described in rule 2.519(d), ITAC determined the proposed amendments should strike an appropriate balance between privacy and access to provide private criminal defense counsel with access on par with public defenders. ITAC seeks specific comments on this issue, however.

Limiting remote access by public defenders

Instead of expanding the scope of electronic records that private counsel can access remotely, one alternative to provide parity of remote access with public defenders would be limiting the scope of public defenders' remote access to only those clients represented by the public defender's office.

ITAC considered this approach undesirable for a few reasons. First, it may be impractical and controversial, especially for courts that have already established remote access for public defenders. Second, it would also create a new parity issue: all criminal defense attorneys would have remote access that is less than what prosecutors could have under the rules. Even if prosecutors were limited to the cases they were prosecuting, they would practically have greater access than defense counsel in each county because there is one district attorney's office in each county but multiple defense counsel. Thus, remote users from the district attorney's office would be able to access significantly more criminal electronic records than public and private defense counsel. As such, there would be a parity issue since district attorneys would have the ability to remotely access criminal electronic records in cases of witnesses or codefendants, while defense counsel would not necessarily have the same access. Accordingly, this was the least desirable alternative to the proposed amendments and the status quo.

Providing attorneys remote access to any electronic record they could access at the courthouse

ITAC considered whether there was a broader issue of providing attorneys remote access to *any* electronic records that they could access at the courthouse. This also raised concerns about remote access versus practical obscurity. Ultimately, ITAC decided to keep the scope of the proposal limited to address the specific problem CACJ identified, but may explore broader access to other case types in the future with the participation of other Judicial Council advisory committees.

Fiscal and Operational Impacts

While the proposed rule amendment would authorize courts to allow remote access to electronic criminal records by private criminal defense counsel, courts would need to implement appropriate technological updates in their systems to accomplish it and provide training to staff about the update. While the aim of the remote access rules is for courts to provide remote access to certain users, including private counsel, the rules recognize that courts have varying financial

[9] Rules Prof. Conduct, rule 3.3 (candor toward tribunal), *https://www.calbar.ca.gov/Portals/0/documents/rules/Rule_3.3-Exec_Summary-Redline.pdf* (as of Feb. 15, 2022).

means, security resources, or technical capabilities to allow them to implement remote access systems.[10] Thus, implementation is only required to the extent it is feasible for a court to do so.[11]

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- If the rule is *not* amended, in what ways would that impact the quality of a defendant's representation for a defendant represented by private counsel?
- Does the proposal adequately strike a balance between privacy and remote access to criminal electronic records by criminal defense attorneys? If not, why not?
    - Should remote access be broader than what the proposal provides?
    - Should remote access be narrower than what the proposal provides?
- Should there be any additional consequences identified in the rule for failure to comply with the terms of remote access? If yes, what consequences should be included?

The advisory committee also seeks comments from *courts* on the following cost and implementation matters:

- Would the proposal provide cost savings? If so, please quantify.
- What would the implementation requirements be for courts—for example, training staff (please identify position and expected hours of training), revising processes and procedures (please describe), changing docket codes in case management systems, or modifying case management systems?
- Is implementation feasible at present or in the near future? If not, what are the barriers to implementation?

Attachments and Links

1. Cal. Rules of Court, rule 2.519, at pages 6–7
2. Administrative Office of the Courts Manager Charlene Hammitt and Special Consultant Victor Rowley, memorandum to Chief Justice Ronald M. George and Members of the Judicial Council, Dec. 10, 2001, regarding proposed rules on electronic access to court records, at pages 8–23
3. Link A: California Rules of Court, Title 2, *https://www.courts.ca.gov/cms/rules/index.cfm?title=two*

[10] Rule 2.516.

[11] Rule 2.516.

Rule 2.519 of the California Rules of Court would be amended, effective January 1, 2023, to read:

Rule 2.519. Remote access by a party's attorney

(a) Remote access generally permitted

(1) A party's attorney may have remote access to electronic records ~~in the party's actions or proceedings~~ under this rule or under rule 2.518. If a party's attorney gains remote access under rule 2.518, the requirements of rule 2.519 do not apply.

(2) If a court notifies an attorney of the court's intention to appoint the attorney to represent a party in a criminal, juvenile justice, child welfare, family law, or probate proceeding, the court may grant remote access to that attorney before an order of appointment is issued by the court.

(b) Level of remote access

(1) A party's attorney may be provided remote access to the same electronic records in the party's actions or proceedings that the party's attorney would be legally entitled to view at the courthouse.

(2) An attorney representing a party in a criminal action may be provided remote access to any electronic criminal records that the attorney would be legally entitled to view at the courthouse.

(c) Terms of remote access applicable to an attorney who is not the attorney of record

Except as provided in subdivision (b)(2), an attorney who represents a party, but who is not the party's attorney of record in the party's actions or proceedings, may remotely access the party's electronic records, provided that the attorney:

(1) Obtains the party's consent to remotely access the party's electronic records; and

(2) Represents to the court in the remote access system that he or she has obtained the party's consent to remotely access the party's electronic records.

(d) Terms of remote access applicable to all attorneys

(1) ~~A party's~~ An attorney may remotely access the electronic records only for the purpose of assisting ~~the~~ a party with ~~the~~ that party's court matter.

(2) ~~A party's~~ An attorney may not distribute for sale any electronic records obtained remotely under the rules in this article. Such sale is strictly prohibited.

(3) ~~A party's~~ An attorney must comply with any other terms of remote access required by the court.

(4) Failure to comply with these rules may result in the imposition of sanctions, including termination of access.

Judicial Council of California
Administrative Office of the Courts

Information Services Division
455 Golden Gate Avenue ◆ San Francisco, CA 94102-3660
Telephone 415-865-7400 ◆ Fax 415-865-7496 ◆ TDD 415-865-4272

RONALD M GEORGE
Chief Justice of California
Chair of the Judicial Council

WILLIAM C VICKREY
Administrative Director of the Courts

RONALD G OVERHOLT
Chief Deputy Director

PATRICIA YERIAN
Director
Information Services Division

TO:	Chief Justice Ronald M. George Members of the Judicial Council
FROM:	Charlene Hammitt, Manager Victor Rowley, Special Consultant
DATE:	December 10, 2001
SUBJECT/ PURPOSE OF MEMO:	Proposed Rules on Electronic Access to Court Records

CONTACT FOR FURTHER INFORMATION:	**NAME:**	**TEL:**	**FAX:**	**EMAIL:**
	Charlene Hammitt	415-865-7410	415-865-7497	charlene.hammitt@jud.a.gov

QUESTION PRESENTED

Why should the rule prohibit remote electronic access (other than to the register and calendar) in case types other than civil?

REASONS FOR PRECLUDING REMOTE ACCESS TO SPECIFIC CATEGORIES OF CASE FILES

Proposed rules 2070-2076 require courts to provide electronic access to general information about court cases and prohibit them from providing access to case files in certain types of cases.

Rule 2073(b) would require courts to provide remote access to registers of actions (as defined in Government Code section 69845) and calendars when they can feasibly do so.

Rule 2073(c), however, would require courts to restrict access to electronic versions of the documents and other records that are found in case files. Under this rule, only case files in civil cases would be available remotely. Files in other types of cases, which are listed in 2073(c), would not be accessible remotely at this time.

The proposed rules represent an initial approach to providing remote access to electronic case files that are likely to contain sensitive and personal information. Electronic records in all case types could be available through terminals at the courthouse. This approach provides them the same de facto privacy protection traditionally afforded paper records. The United States Supreme Court has characterized this protection as a "practical obscurity" that is attributable to the relative difficulty of gathering paper files. See *United States Dep't of Justice* v. *Reporters Committee for Freedom of the Press* 489 U.S. 749 [109 S.Ct. 1468, 103 L.Ed.2d 774].

Delivery of court records on the Internet constitutes publication and typically facilitates republication. With the exception of docket information, trial courts generally have not been publishers of case records. Electronically published data can be easily copied disseminated, and its dissemination is irretrievably beyond the court's control. Publication of court records on the Internet creates a much greater threat to privacy interests than does access to paper records, or access to electronic records through terminals at the courthouse.

The case-types set out in rule 2073 (c) would be precluded from remote access for the following reasons:

- *Sensitive personal information unrelated to adjudication.* Courts sometimes collect sensitive personal information that has no bearing on the merits of a case but that assists the court in contacting parties or in record keeping. Such information could include unlisted home telephone numbers, home addresses, driver's license numbers, and Social Security numbers. Before such information is published on the Internet, the Judicial Council should survey trial courts to identify the sensitive or personal information they collect, determine whether or not this information is essential to workload management, and then consider how to protect such information when it is legitimately needed.

- *Privacy of involuntary participants.* Individuals who are sued, subpoenaed, or summoned for jury duty are involuntary participants in legal proceedings and may be

compelled to provide the court with sensitive personal information. As records custodians, courts should proceed with caution in publishing such information, as it has relatively little relevance to the public's ability to monitor the institutional operation of the courts but relatively great impact on the privacy of citizens who come in contact with the court as defendants, litigants, witnesses, or jurors. Publication of sensitive financial, medical, or family information provided by involuntary court participants could, for instance, harm individuals by holding them up to ridicule, damaging their personal relationships, and foreclosing business opportunities.

- *Investigations in criminal cases.* The Federal Judicial Conference[1] in September 2001 adopted a policy that makes criminal cases unavailable remotely for a two-year period. The Judicial Conference identified two reasons for this exclusion of criminal cases. First, electronic publication of criminal case records could jeopardize investigations that are under way and create safety risks for victims, witnesses, and their families. Second, access to preindictment information, such as unexecuted arrest and search warrants, could severely hamper law enforcement efforts and put law enforcement personnel at risk. These reasons would apply to the proposed California policy as well.

- *Criminal histories.* Allowing remote electronic access to criminal cases would greatly facilitate the compilation of individual criminal histories, in contravention of public policy as established in statute. (See *Westbrook v. City of Los Angeles* (1994) 27 Cal.App.4th 157 [court note required to provide to public database containing criminal case information].) For this reason, the Attorney General supports excluding criminal cases from remote electronic access:

  > Our principal concern is with criminal records and the threat that the electronic release of these records poses to individual privacy and to the legislative and judicial safeguards that have been created to insure that only accurate information is disclosed to authorized recipients. (See, e.g., Penal Code sec. 11105.) The

---

[1] "The federal court system governs itself on the national level through the Judicial Conference of the United States The Judicial Conference is a body of 27 federal judges It is composed of the Chief Justice of the United States, who serves as the presiding officer, the chief judges of the 13 courts of appeal, the chief judge of the Court of International Trade, and 12 district judges from the regional circuits who are chosen by the judges of their circuit to serve terms of three years The Judicial Conference meets twice yearly to consider policy issues affecting the federal courts, to make recommendations to Congress on legislation affecting the judicial system, to propose amendments to the federal rules of practice and procedure, and to consider the administrative problems of the courts " See http://www.uscourts gov/understanding_courts/89914 htm

electronic dissemination of criminal records is a tremendous danger to individual privacy because it will enable the creation of virtual rap sheets or private databases of criminal proceedings which will not be subject to the administrative, legislative or judicial safeguards that currently regulate disclosure of criminal record information. (Letter from Attorney General Daniel E. Lungren commenting on draft rules (March 6, 1997); See letter from Attorney General Bill Lockyer (Dec. 15, 2000), reaffirming position taken in March 6, 1997 letter.)

- *Risk of physical harm to victims and witnesses.* The safety of victims and witnesses could be compromised if courts were to publish their addresses, telephone numbers, and other information that would allow them to be located. Such risk is perhaps most common in criminal and family cases.

- *Fraud and identity theft.* Although sensitive personal information, such as Social Security and financial account numbers, may already be available in paper files at the courthouse, its "practical obscurity" has provided it with de facto privacy protection. Publishing such information on the Internet exposes it to a substantial risk of criminal misuse. Participation in court proceedings, whether voluntary or involuntary, should not expose participants to such victimization.

- *Determination of reliability.* Ex parte allegations, particularly in family cases, present a problem in that they may be skewed by self-interest and subsequently determined to be unreliable. Although such allegations could be read in case files at the courthouse, the physical demands of accessing such files would afford them "practical obscurity." Courts should not broadcast ex parte allegations on the Internet until there are policies and procedures to address the problems of unvetted ex parte allegations.

- *Statutory rehabilitation policies.* Various sections of the Penal Code allow for sealing of a defendant's criminal record provided that certain conditions are met. Such sealing does not occur by operation of law; see for instance the entries on arrest or conviction for marijuana possession and the record of a "factually innocent" defendant in Table 1. If such information is published before conditions for sealing are met, the publication would make the subsequent sealing ineffectual and thus thwart the rehabilitative intent of the authorizing legislation. Admittedly, information could be published from files accessed at the courthouse, but the "practical obscurity" of such files has lessened the likelihood of publication and reduced the risk of thwarting rehabilitation policies. Publication on the Internet would make it difficult to implement such policies.

- *Tools to apply confidentiality policies.* By statute, courts are obligated to protect confidential information in many types of case records, including some of the types of case records specified in rule 2073(c) (see Table 1). This obligation may be absolute or defined by statutorily set or judicially determined time limits. Courts have traditionally met these obligations on an ad hoc basis, as individual case records have been requested at the courthouse. To respond in a responsible manner to remote electronic requests, courts would need to meet these obligations by applying appropriately protective criteria to all records, not only those that are requested but those that might be. Courts simply do not have staff who can review and monitor all records to make them available for remote electronic access. They will need to use automated tools to address the review and monitoring problem. Effective tools should be based on standards. Standards should then be applied by case management systems. Until these standards can be developed and applied by case management systems, the proposed rules would make specified case types unavailable by remote electronic access.

- *Inadvertent exposure of sensitive or personal information* Parties to the excepted case types (particularly family law) who are unaware that sensitive or personal information included in court filings is publicly accessible will also be unaware they can take steps to protect such information, by requesting a sealing or protective order. For example, in family law proceedings, it is not unusual for litigants to attach copies of their tax returns to their filings, even though tax returns are made confidential by statute. Similarly, in family law proceedings, allegations of abuse are not uncommon; however, litigants may not be aware that there are procedures for limiting public access to this highly sensitive and personal information to protect not only their own privacy, but that of their minor children. The exceptions to remote access in rule 2073 (c) afford time for the Judicial Council to consider how the privacy interests of litigants, particularly the self-represented, might be protected before courts electronically publish case files that include sensitive or personal information that litigants have inadvertently disclosed.

Policy development. While the proposed rules encourage courts to use technology to facilitate access to court records (in accordance with long-term goals of the judicial branch), they do so cautiously, providing breathing room while privacy issues and records policies are more thoroughly reexamined at state and federal levels. The rules allow remote access to civil case files. Civil cases do present some of the same privacy

concerns discussed above, but generally to a lesser degree than in the types of case records that are unavailable under 2073(c). The courts' experiences with remote access to civil cases will guide the council's policy-making in the future. This incremental approach allows further debate and experimentation. Such an approach is in line with the approach adopted by the Judicial Conference of the United States and other states.

Proposed Rule 2073(c)

RECORDS NOT AVAILABLE BY REMOTE ELECTRONIC ACCESS

Under proposed Rule 2073(c), the public would be provided with electronic access to court records in specified case types only at the courthouse and not remotely, pending the development and implementation of software standards that enable the courts to meet their legal obligations to protect confidentiality and privacy. This table illustrates the confidentiality and privacy issues that the courts must resolve before providing such remote electronic access to the public.

Case type	*Record type*	*Restricted data*	*Legal authority*	*Comment*
CIVIL				
Civil or criminal	Subpoenaed business records	Entire record	Evid Code § 1560(d) (confidential until introduced into evidence or entered into record)	As with court records generally, these records are not accessible by public unless and until relied on by court as part of adjudicative process See *Copley Press Inc v Superior Court* (1992) 6 CA4th 106, 113-15 (public right of access to court records does not apply to all of court's records and files, but only to records that officially reflect work of court)
All cases involving fee waiver application	Fee waiver application	Entire record	Cal Rules of Court, rule 985(h) (records of application to proceed without paying court fees and costs are confidential)	Purpose is to prevent disclosure of applicant's financial information
All cases involving attachment	Records in attachment action	Entire record	Code Civ Proc § 482 050(a) (attachment action records are confidential for 30 days from filing complaint or return of service, on plaintiff's request).	
All cases involving garnishment	Judicial Council forms 982 5 (11S) and 982 5 (14S)	Entire form	Judicial Council forms 982 5 (11S) and 982 5 (14S)	Purpose is to prevent disclosure of debtor's Social Security Number (SSN)
Unlawful detainer	Register of Actions	Case title, date of commencement, memorandum of	Code Civ Proc § 1162(a) (in certain unlawful detainer actions, Register of Actions unavailable for 60 days from	

		every subsequent proceeding and date (see Gov Code § 69845)	filing of complaint)	
CIVIL HARASSMENT				
Harassment generally		Address and telephone number of applicant for restraining order.	CCP § 527 6 (requires showing of unlawful violence, credible threat of violence, or course of conduct resulting in "substantial emotional distress," including stalking)	No explicit statutory authority, but publication of the restricted information might facilitate further harassment Analogous to authority given to court under Fam Code to prohibit disclosure of identifying information in proceeding under Domestic Violence Prevention Act (see below)
Domestic Violence		Address and telephone number of applicant for restraining order and or his or her minor children.	Fam Code § 6322 5 (court may issue ex parte order prohibiting disclosure of address or other identifying information of a party, child, parent, guardian, or other caretaker of child in proceeding under Domestic Violence Prevention Act)	Publication of the restricted information might facilitate further harassment
CRIMINAL				
	Grand jury proceedings		Pen Code § 938 1(b) (transcript not subject to disclosure until 10 days after delivery to defendant or attorney, subject to specified conditions)	Records not public unless indictment returned
	Search warrants and affidavits	Entire record until return of service or 10 days after issuance, whichever is first	Pen Code § 1534(a) (these records are confidential for time period specified)	
	Police reports	Address or telephone number of victims, witnesses	Pen Code § 1054 2 (no attorney may disclose unless permitted to do so by the court after a hearing and a showing of good cause)	Conforms to policy of Pen Code § 841 5 (no law enforcement officer or employee of law enforcement agency shall disclose to any arrested person, or to any person who may be a defendant in a criminal action, address or telephone number of victim or witness in alleged offense)
	Pre-sentence	Entire record	Pen Code § 1203 05 (pre-sentence	Publication on Internet would effectively be

	probation report		probation report is confidential after 60 days from sentencing or granting of probation and under certain other conditions)	permanent and thus thwart policy behind making record unavailable after 60 days
	Pre-sentence diagnostic report	Entire record	Pen Code § 1203 03 (report is confidential)	Unavailable as public record in any form absent change in legislative policy
	Defendant's statement of assets	Entire record	Pen Code § 1202 4 (mandatory Judicial Council form (CR-115) is confidential)	Purpose is to prevent disclosure of defendant's financial information
	Criminal history information	Summaries of criminal history information	Summaries of criminal history information are confidential (*Westbrook v Los Angeles* (1994) 27 CA4th 157, 164, Pen Code §§ 11105, 13300-13326) Public officials have duty to preserve confidentiality of defendant's criminal history (*Craig v Municipal Court* (1979) 100 CA3d 69, 76)	Court in *Westbrook* noted adverse impact of disseminating this information with its potential for frustrating policies permitting subsequent sealing or destruction of records, or limiting dissemination of similar records by other criminal justice agencies (pp 166-67) Pen Code § 11105 limits access to state summary criminal history information to public agencies and others given express right of access by statute Pen Code § 13300 contains similar limitations on public access with respect to local summary criminal history information
	Arrest or conviction for marijuana possession	All records except for transcripts or appellate opinions, see Health & Saf Code § 11361 5(d)	Health & Saf Code §§ 11361 5-11361 7 (generally, records of arrest or conviction for marijuana possession to be destroyed two years from date of arrest or conviction)	Publication on Internet would effectively be permanent and thus thwart policy behind sealing after sentencing
		Any information	42 CFR 2.12 (restricts disclosure of patient identity in federally assisted alcohol or drug abuse rehabilitation program)	Publication is antithetical to goal of rehabilitation
	Record of "factually innocent" defendant	Entire record	Pen Code §§ 851 8, 851 85 (on acquittal, or if no accusatory pleading is filed or, after filing, there is a judicial determination that defendant was	Publication on Internet would effectively be permanent and thus thwart policy behind sealing

			"factually innocent" of the charges, court records, including arrest records may be sealed)	
	Indigent defendant requests	Indigent defendant's in forma pauperis records and request for experts in capital case	Cal Rules of Ct 985(h) (indigent defendant's in forma pauperis records are confidential) and Pen Code § 987 9 (request for experts in capital case are confidential)	Purpose of Rule 985(h) is to prevent disclosure of defendant's financial information Purpose of sec 987 9 is to preserve confidentiality of defense
	Plea based on insanity or defense based on defendant's mental or emotional condition	Entire record	Evid Code § 1017 (psychotherapist appointed by order of court on request of lawyer for defendant in criminal proceeding, to provide lawyer with information to advise defendant whether to enter or withdraw plea based on insanity or to present defense based on mental or emotional condition)	Purpose is to preserve confidentiality of defense
	Reports concerning mentally disordered prisoners	Entire record	Pen Code § 4011 6 (reports to evaluate whether prisoners are mentally disordered are confidential	
	Victim/witness information	Specified victim personal identifying information and victim impact statements	Gov Code § 6254(f)(2) and Pen Code § 293 (in specified abuse and sexual assault cases, victim's name and address, and the offense, confidential on victim's request). Pen. Code § 293 5(a) (at request of victim of certain sexual offenses, court may order that victim's identity in all records be either Jane Doe or John Doe, on finding that order is reasonably necessary to protect victim's privacy and will not unduly prejudice prosecution or defense) Pen. Code § 1191.15 (victim impact	Purpose is to protect victim's privacy

10

			statements are confidential before judgment and sentencing and may not be copied After judgment and sentencing, statement must be made available as public record of court)	
Misdemeanor proceedings	Dismissal of accusatory pleading and setting aside of guilty verdict		Pen Code § 1203 4a (misdemeanor proceedings resulting in conviction may be modified on petition and proof that one year has elapsed from date of judgment, sentence has been fully complied with, and no other crimes have been committed)	Publication is antithetical to goal of rehabilitation
Fines, fees, forfeitures	Any record containing Social Security Number (SSN)	Social Security Number	Gov Code § 68107 (court may order criminal defendant on whom fine, forfeiture, or penalty is imposed to disclose social security number to assist court in collection, but number is not a public record and is not to be disclosed except for collection purposes), see also 42 U S C § 405(c)(2)(C)(viii) (I)	Purpose is to prevent disclosure of defendant's Social Security Number (SSN)
FAMILY				
Child or spousal support	Tax return	Entire record	Fam Code § 3552 (parties' tax returns filed in support proceedings must be sealed)	Unavailable as public record in any form absent change in legislative policy
Child custody	Custody evaluation report	Entire record	Fam Code § 3111 (report is available only to court, parties, and their attorneys)	In general, these records are made confidential to protect privacy of parties and their minor children
	All, when noncustodial parent is registered sex offender, or convicted of child	Custodial parent's place of residence and employment, and child's school	Fam Code § 3030(e) (this information may not be disclosed unless court finds that disclosure would be in child's best interest)	

	abuse, child molestation, or rape that resulted in child's conception		
Other	Records in conciliation proceedings	Entire record	Fam Code § 1818(b) (files of family conciliation court shall be closed)
	Records in action under Uniform Parentage Act (UPA)	All records, except for final judgment	Fam Code § 7643(a) (records are subject to public inspection only in exceptional cases, on court order for good cause shown).
	Petition and probation or social services report in proceeding to terminate parental rights	Entire record	Fam Code § 7805 (records are to be disclosed only to court personnel, the parties, and persons designated by the judge)
	Adoption records	Entire record	Fam Code § 9200(a) (judge may not authorize public inspection except in exceptional circumstances and for good cause "approaching the necessitious")
	Support enforcement, child abduction	Entire record	Fam Code § 17212 (records generally confidential with specified exceptions)
	Support enforcement under Uniform Interstate Family Support	Address of child or party or other identifying information	Fam Code § 4926 (on finding that health, safety, or liberty of party or child would be unreasonably put at risk by disclosure of identifying information, court shall order that address of child or party or other identifying information not be disclosed in any pleading or other document filed

	Act		in proceeding under Act)	
	Confidential Counseling Statement (Marriage)	Judicial Council Form 1284	Judicial Council Form 1284	
GUARDIANSHIP, CONSERVATORSHIP				
	Confidential Guardian Screening Form (Probate Guardianship)	Entire Judicial Council Form GC-212	Prob Code § 1516, Cal Rules of Court, rule 7 1001	
	Confidential Conservator Screening Forms (Probate Conservatorship)	Entire Judicial Council Forms GC-314 and GC-312	Prob Code § 1821(a), Cal Rules of Court, rule 7 1050	
	Report and recommendation re proposed guardianship	Entire record	Prob Code § 1513(d) (report of investigation and recommendation concerning proposed guardianship is confidential)	Unavailable as public record in any form absent change in legislative policy
	Report and recommendation re proposed conservatorship	Entire record	Prob Code § 1826(n) (report of investigation and recommendation concerning proposed conservatorship is confidential, except that court has discretion to release report if it would serve conservatee's interests)	
	Report arising from periodic review of conservatorship	Entire record	Prob Code § 1851(e) (report is confidential, except that court has discretion to release report if it would serve conservatee's interests)	
	Periodic accounting of assets in estate or	Accounting containing ward's or conservatee's	Prob Code § 2620(d) [AB 1286, 1517] (accounting containing this information should be filed under seal)	

	ward or conservatee	Social Security number or any other personal information not otherwise required to be submitted to court		
JUROR RECORDS				
	Juror questionnaires and personal identifying information	Jurors' names, addresses, and telephone numbers	Code Civ Proc § 237 (juror personal identifying information after verdict in criminal case, to be confidential) *Bellas v Superior Court* (2000) 85 CA4th 636, 646 (jurors' responses to questionnaires used in voir dire are accessible by public unless judge orders them to be sealed) *Townsel v Superior Court* (1999) 20 C4th 1084, 1091 (trial courts have inherent power to protect juror safety and juror privacy) *Copley Press, Inc v Superior Court* (1991) 228 CA3d 77, 88 (public should not be given access to personal information furnished to determine juror qualification or necessary for management of the jury system, but not properly part of voir dire, *e g*, the prospective juror's telephone number, SSN, or driver's license number) See also Cal Rules of Court, rule 33 6 (sealing juror-identifying information in record on appeal).	Do courts have an obligation to protect the privacy of these nonparties to the proceeding?
JUVENILE				
All	All	Entire record	Welf & Inst Code § 827 and Cal Rules of Court 1423 (access to case files in juvenile court proceedings is generally restricted), Pen Code § 676 (certain violent offenses excepted)	General purpose behind confidentiality of these records is to promote rehabilitation of juvenile offenders

14

	Adult court criminal records		Pen Code § 851 7 and Welf & Inst Code § 707 4 (adult court criminal records involving minors that do not result in conviction to be sent to juvenile court, to obliterate minor's name in adult court index or record book) Pen Code § 1203 45 (minor would qualify for judgment modification as a probationer or misdemeanant)	
	Record of "factually innocent" defendant	Entire record, including arrest record	Pen. Code § 851 85 (any criminal proceedings, after acquittal plus judicial finding of factual innocence)	
	Judgments		Pen. Code § 1203 4 (criminal judgments may be modified for convicted probationers after successful completion of probationary period) or Pen Code § 1203 4a (criminal judgments may be modified for convicted misdemeanants after one year and successful completion of sentence)	
	All records, papers, and exhibits in the person's case in the custody of the juvenile court (see Welf. & Inst Code §781)	Entire juvenile court record, minute book entries, and entries on dockets, and any other records relating to the case	Welf & Inst. Code §781 (juveniles declared wards of the court may on petition have their juvenile court records (including those made public by Welf & Inst Code § 676) sealed five years after the jurisdiction of the court ceases or the juvenile reaches 18, if there are no subsequent convictions involving felonies or moral turpitude, and there is a finding of rehabilitation)	
MENTAL HEALTH				

15

Civil and criminal	Mental health service records	Entire record	Welf & Inst Code §§ 5328-5330 (specified records confidential and can be disclosed only to authorized recipients, including records related to the Dept. of Mental Health; Developmental Services; Community Mental Health Services, services for developmentally disabled, voluntary admission to mental hospitals and mental institutions)	Publication on Internet would effectively be permanent and thus thwart policy behind sealing after sentencing
	Developmentally Disabled Assessment Reports	Entire record	Welf & Inst Code § 4514 (Developmentally Disabled Assessment Reports, to be sealed after sentencing)	Publication on Internet would effectively be permanent and thus thwart policy behind sealing after sentencing

16

SOCIAL SECURITY NUMBERS By statute SSNs are required in the following court proceedings

(1) The judgment debtor's SSN (if known to the judgment creditor) must be set forth on the abstract of judgment CCP § 674(a)(6)
(2) The application for an earnings withholding order must include the judgment debtor's SSN (if known to the judgment creditor CCP § 706 121(a) The earnings withholding order and the employer's return must also include this SSN if known CCP §§ 706 125(a) (order), 706 126(a)(3) (return)
(3) As noted above with regard to criminal cases, courts are authorized to collect SSNs from criminal defendants with fines, forfeitures, or penalties imposed, but these numbers are not to become public records and are not to be disclosed except for collection purposes Govt Code § 68107

In civil and bankruptcy cases in the federal courts, only the last four digits of a party's SSN should be set forth in any document filed with the court See http //www uscourts gov/Press_Releases/att81501 pdf