Stanford Law School
Stanford Criminal Justice Center

Criminal Justice Information Sharing:

A Legal Primer for Criminal Justice Practitioners in California

W. David Ball

Robert Weisberg

Stanford Law School
559 Nathan Abbott Way
Stanford. CA 94305

December 2010

CRIMINAL JUSTICE INFORMATION SHARING: A LEGAL PRIMER FOR CRIMINAL JUSTICE PRACTITIONERS IN CALIFORNIA

W. David Ball[*] *& Robert Weisberg*[*]

ABSTRACT

California criminal justice agencies need access to data in order to provide security, health care treatment, and appropriate programming, as well as to coordinate these activities with other agencies. By the same token, outside agencies—whether criminal, social service, or non-governmental—could often do their jobs more effectively with access to information generated or retained within particular criminal justice agencies. Criminal justice realignment under AB 109 has only heightened the need for inter-agency data sharing and cooperation, yet there continue to be misunderstandings about the legal framework surrounding information exchange.

This Article aims to provide a basic, practical background on the legal rules relevant to information exchange, highlighting under what circumstances—and with whom—criminal justice agencies may share, must share, or must not share their information. The Article's basic conclusion is that criminal justice data sharing is enabled by the existing legal regime.

[*] Assistant Professor, Santa Clara School of Law; Research Fellow, Stanford Criminal Justice Center.

[*] Edwin E. Huddleson, Jr., Professor of Law, Stanford Law School., Faculty Co-Director, Stanford Criminal Justice Center.

This project, while the work of the named authors, also serves as a report of the Stanford Criminal Justice Center (SCJC), as part of its analysis of the contemporary criminal justice system in California. In particular, it was developed in response to the very practical concerns of officials and policymakers from all branches of California government who attended meetings at SCJC and expressed the desire for the type of guidance this Primer aims to provide. While the errors remain the authors', much of the heavy lifting on the research was conducted by the fabulous team of Research Assistants: Che Banjoko, Masha Hansford, Alexandra Lampert, Jacob Russell, Scott Schaeffer, and Rebecca Weber.

INTRODUCTION

California criminal justice agencies need access to data in order to provide security, health care treatment, and appropriate programming, as well as to coordinate these activities with other agencies. By the same token, outside agencies—whether criminal, social service, or non-governmental—could often do their jobs more effectively with access to information generated or retained within particular criminal justice agencies. For example, knowing that an arrestee is mentally ill could assist a jail with his classification, housing, and medical care; similarly, knowing the risk status of a released prisoner could help local community supervision prepare for support services and supervision. Coordination of information exchange involves a number of technical and organizational challenges, but there is also considerable uncertainty about governing law. So, while the need for information is great, in the absence of legal guidance, some agencies are understandably reluctant to share information. They are unsure about whether it will expose them to civil liability under statutes protecting confidentiality or other legal rules. In regard to the many varied categories of individual information they handle, agency officials often ask: When am I *forbidden* to disclose information? When am I *allowed* to disclose information (and to whom)? When am I *required* to disclose information (and to whom)?

This Article is designed to address and alleviate these concerns, to

help state and local officials understand the most important and widely applicable legal doctrines that determine their responsibilities in handling information developed or collected in the many stages of criminal justice. Readers should, however, note that this Primer is only a starting point: its goal is to provide a broadly accurate overview of the issues, *not* to give legal advice for specific governmental decisions. Therefore, we urge readers to consult with an attorney before adopting any specific new policies on information sharing or making specific decisions about information-sharing in any sensitive matter.

EXECUTIVE SUMMARY

A review of the legal doctrines governing information-sharing in criminal justice leads to one overall conclusion: California law contains a strong mandate for robust information-sharing among agencies involved in any substantial way with criminal justice, and criminal justice information-sharing faces few legal barriers—surely far fewer than many officials tend to believe as a matter of common intuition or perception. So long as agencies exercise care in the security and confidentiality of the information they exchange, they will, in general, not be exposed to statutory or civil liability for information transfers that serve reasonable institutional purposes.

One should read the entire Primer to get a sense of this legal area as a whole, but the Primer has also been divided into topic headings for easy reference. The following key summary points reflect the organization of the Primer:

1. Sharing summary information among criminal justice agencies is a "safe harbor." Agencies should feel comfortable sharing this information with other criminal justice agencies, provided the sharing is done with appropriate safeguards. These safeguards already govern the use of criminal justice data. That is, changes wrought by either technology or realignment do not change the rules. As long as agencies continue to follow the rules with which they are (or should be) already familiar, there is nothing new—and uncertain—about exchanging such information electronically or under the rubric of realignment. Statutes and agency regulations govern who can properly use data in the California Law Enforcement Telecommunications System (CLETS). Those statutes and regulations extend data privileges to those with a "need to

know" and those with a "right to know" in law enforcement. Agencies that share data maintained in separate case management systems, where those systems may include some CLETS derived information, should follow the security requirements (such as secure network and limited access) for CLETS secondary dissemination. Neither intellectual property nor security concerns should prohibit this increased sharing, so long as existing security policies are incorporated into any additional sharing procedures. Moreover, this principle applies to sharing with federal law enforcement authorities as well as sharing with other state or local authorities.

2. Medical information disclosure laws—the federal Health Insurance Portability and Accountability Act (HIPAA) and the California Confidentiality of Medical Information Act (CMIA)—do not pose great obstacles to information sharing. HIPAA is very weakly enforced and has many relevant exceptions. In practice, the CMIA governs and should accommodate information sharing. The California Constitution and Information Practices Act add potential complexities, but most of the relevant considerations for an information sharing system are in CMIA and HIPAA.

3. Because of prohibitions contained in the California Constitution, government agencies need to establish very clear procedures controlling disclosure of information from or about crime victims.

4. Government agencies hoping to *prevent* disclosure of records under the California Public Records Act (CPRA) should recognize that, on the whole, courts construing the CPRA will tend to favor public disclosure.

5. In regard to criminal investigations, employees of police departments and the judicial branch are not likely to suffer any consequences for relying on inaccurate data in executing search warrants, so long as the errors leading to the unlawful search were truly negligent. But where errors leading to unlawful searches are widespread and systemic, evidence resulting from the unlawful search may be suppressed, and employees or departments may be subject to civil liability. The rare but successful instances of § 1983

claims for inaccurate data strongly suggest that agencies implement protocols that allow individuals to check and report errors in their records, particularly where the records are widely shared and affect that individual's ability to take advantage of public and private services.

6. Confidential information in the hands of government officials may trigger a defendant's due process right to discovery of potentially exculpatory evidence. District Attorneys, who are legally bound to share exculpatory information with defendants, may be responsible for disclosing such information that is held by other agencies, if that other agency's system or operation is sufficiently integrated with that of the prosecutor's office.

7. The risks of civil liability for defamation or invasion of privacy from the sharing of criminal justice information are very small. Broad protections for governmental officials and agencies acting in good faith serve to insulate them against lawsuits for wrongful disclosure, at least in the absence of intentional or malicious conduct.

***

This Article proceeds as follows. Part I gives an overview of the data sharing landscape. This information is included largely for non-practitioners, as the information it contains is common knowledge to those who work within California's criminal justice system. Part II discusses the "safe harbor" case of criminal justice agencies sharing summary criminal justice information among themselves. The legal rules, in general, promote this activity, provided that certain basic safeguards (already in place) are followed. Part III discusses issues related to medical information governed by HIPAA (and, to a lesser extent, the California state equivalent), concluding that what issues there are would be easily solved. Part IV briefly examines the special case of information about victims, which is protected under Marsy's Law. Part V discusses when criminal justice agencies must disclose information to private parties under the California Public Records Act. Part VI discusses issues relating to investigation and litigation, specifically what might happen if law enforcement relies on inaccurate data when conducting its investigation, and what duties prosecutors have to disclose information to the defense. It also touches on how evidentiary privileges might come into play with greater information

exchange. Finally, Part VII discusses liability, concluding that there is little scope for claims of defamation or invasion of privacy.

I. THE DATA-SHARING LANDSCAPE

This section provides a rudimentary survey of the California data-sharing landscape. Most practitioners, who will already be familiar with the main mechanisms of data exchange, can skip this section.

Information exchange in California takes place under a variety of forms: CLETS, case management systems such as COPLINK, and Regional Information Sharing Systems. Nearly every official working in California's criminal justice system should be familiar with the operation of the California Law Enforcement Telecommunications System (CLETS), the backbone of state criminal justice information.[1] In addition, most practitioners will be familiar with case management systems (CMS's—also known as Records Management Systems, or RMS's), of which the most popular is COPLINK. These systems collect data electronically and can share this information—to varying degrees, with varying ease—with outside agencies. Finally, agencies also regularly share data through joint agreements[2] or under regional arrangements that disseminate data across many different jurisdictions, most notably through Regional Information Sharing Systems (RISS). Each of these three types of data sharing arrangements will be discussed in turn.

CLETS. CLETS is a "high-speed communications application" that offers law enforcement agencies access to dozens of unique databases with local, state, federal, and international criminal justice information.[3] The state provides each county with hardware and switching center personnel for one CLETS access point.[4] Local agencies must then furnish their own

[1] (As a reference guide, a separate Appendix to this Primer summarizes the basic CLETS operational scheme and gives details on other databases.)

[2] *See* MEMORANDUM OF AGREEMENT AMONG THE INTEGRATED LAW AND JUSTICE AGENCY OF ORANGE COUNTY, THE LOS ANGELES COUNTY SHERIFF'S DEPARTMENT AND KNOWLEDGE COMPUTING CORPORATION (on file with author) (hereinafter MEMORANDUM OF AGREEMENT).

[3] DEPT. OF JUSTICE, STATE OF CALIFORNIA, CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CLETS) 2008 STRATEGIC PLAN §2.7 (Draft Oct. 29, 2008) [hereinafter CLETS Strategic Plan].

[4] Bill Lockyer, California Attorney General, Testimony to the Little Hoover Commission Gov't Technology Hearing (Feb. 24, 2000), *available at* http://www.lhc.ca.gov/lhcdir/gov'tech/LockyerFeb00.pd [hereinafter Lockyer Testimony].

equipment and coordinate with the county in order to connect to this interface.[5] Some agencies, like police departments, can connect directly to CLETS using Computer Aided Dispatch systems to query CLETS from the field.[6] Most other agencies access CLETS through designated terminals, which connect to their county's access point and then relay information to and from the state's databases.

One of the primary uses of CLETS is reporting summary criminal history information, or RAP sheets (Record of Arrest and Prosecution).[7] The California Department of Justice (DOJ) must "maintain state summary criminal history information" and "furnish" it to agencies, including among others state courts, peace officers, prosecuting city attorneys, state district attorneys, public defenders and child welfare agencies "when needed in the course of their duties."[8]

In order to collect this criminal history information, the California Attorney General is required to "procure from any available source, and file for record and report in the offices of the bureau, all . . . information . . . of all persons convicted of a felony, or imprisoned for violating any of the military, naval or criminal laws of the United States."[9] Each sheriff or police chief executive must furnish to the California DOJ daily reports with information about specific misdemeanors and felonies,[10] and also notify the California DOJ when an arrested person is transferred to another agency's custody or "released without having a complaint or accusation filed with a court."[11] State courts are then obliged to report to the California DOJ when they dispose of a case.[12] In Penal Code §§ 13100 -13326, the California Legislature has set detailed standards for the data elements that arresting agencies and courts are required to report to the California DOJ, which the California DOJ maintains in criminal justice databases accessible via CLETS.

CMS. In addition to accessing data via CLETS, many cities and

---

[5] *Id*.

[6] *Id*.

[7] *See* People v. Martinez, 22 Cal. 4th 106 (2000) (allowing admissibility of RAP sheet as evidence of criminal history and discussing statutory framework requiring the CA DOJ to maintain criminal summary information).

[8] CAL. PENAL CODE §11105 (2009).

[9] *Id.* §11101.

[10] *Id.* §11107.

[11] *Id.* §11115.

[12] *Id.* §13151.

counties maintain individual databases, often called "case management systems," tailored to their localities' needs. These systems may operate independently or may link with other agencies. San Francisco County, for example, has integrated all of its criminal justice agencies into one network, called JUSTIS, but does not intend to integrate with any other county.[13] Monterey County, alternatively, attempted to integrate its Criminal Justice Information System with four other counties—Kern, San Joaquin, Marin and San Mateo—but those counties have "never shared data as originally anticipated."[14] Information maintained in local systems is not identical to the information furnished to CLETS—the CA DOJ only requires specific reporting elements, such as records of arrest and case disposition—but local agencies may keep richer records tailored to their local criminal justice system, such as detailed investigation files, court dockets and jail records.

Private vendors, such as COPLINK, specialize in technology that links these case management systems to allow for real-time "complex data searches" across multiple databases in order to "uncover hidden relationships" and aid in investigations.[15] Agencies might favor systems like COPLINK because users can access information via the web from their own computer terminals, instead of being limited to designated CLETS access points. They can also share the information in their individual case management systems, which may contain more detailed records than the California DOJ requests. Agencies wishing to share data with one another in this way often enter into contracts or joint powers agreements,[16] because unlike the myriad information sharing statutes that govern the California DOJ's data requirements, no explicit statutory mechanism exists to provide for information sharing between organizations.

RISS. Data sharing also takes place on a national level. The U.S. Department of Justice, Bureau of Justice Assistance has funded Regional Information Sharing Systems (RISS), which operates via secure intranet "to

---

[13] *See* Office of Budget Analyst, San Francisco, The Justice Information Tracking System (JUSTIS), http://www.sfgov.org/site/budanalyst_page.asp?id=68983.

[14] COUNTY OF MONTEREY, ADDENDUM TO REQUEST FOR PROPOSAL FOR PROGRAM MANAGEMENT SERVICES FOR THE REPLACEMENT AND/OR UPGRADE OF THE JUSTICE INFORMATION SYSTEMS FOR THE COUNTY OF MONTEREY 2 (July 18, 2006), *available at* http://www.co.monterey.ca.us/iss/pdf/Addendum%20RFP%209901.pdf.

[15] COPLINK, http://www.coplink.com (last visited October 19, 2009).

[16] CAL GOV'T CODE §6500 (2009) (Granting authority to enter into Joint Powers Agreements). *See, e.g.*, MEMORANDUM OF AGREEMENT, *supra* note 2.

facilitate law enforcement communications and information sharing nationwide."[17] RISS systems divide the nation into six regional "RISS Intelligence Centers."[18] California is a member of the Western States Information Network, with other member agencies in Alaska, California, Hawaii, Oregon, and Washington, Canada and Guam.[19]

The increased sharing of criminal justice information poses challenges beyond issues of technological integration. Federal, state and local agencies have many security and privacy concerns, raising "[q]uestions such as who owns the data, who has access to the data, [and] who has the right to use the data."[20]

II. DISCLOSURE OF SUMMARY CRIMINAL JUSTICE INFORMATION

Generally, sharing criminal justice information with other criminal justice agencies raises no legal red flags—and, in fact, this sharing is required in some circumstances. There are well-established rules and regulations involving the dissemination of CLETS information—so there is little that should be novel or uncertain about sharing this information. The discussion that follows will be framed by three separate issues: when information must be disclosed, when it may be disclosed, and when it may not be disclosed. The analysis is complicated slightly by the fact that there are two types of criminal justice information—summary information and non-summary information—and that there are several kinds of agencies to whom such information might potentially be disclosed. An analysis of the issues involved in disclosure of information depends first on the kind of information, and second on the agency to which the information is disclosed. This section deals with summary information disclosed to different types of agencies.

The California Penal Code creates a strong foundation for integrated criminal justice information systems and, more generally, formalized information sharing among actors in the criminal justice system.[21] Penal Code Section 13100, in part, recognizes the need for improved access and sharing of information across criminal justice agencies.[22] Penal Code

---

[17] Regional Information Sharing Systems, http://www.riss.net/overview.aspx (last visited October 19, 2009).

[18] *Id.*

[19] *Id.*

[20] Lockyer Testimony, *supra* note 4.

[21] *See* CAL. PENAL CODE § 11105(A)-(S) (2008).

[22] The California Penal Code defines criminal justice agencies as "those

Section 13100(a) explains that "the criminal justice agencies in this state require, for the performance of their official duties, accurate and reasonably complete offender record information."[23] Penal Code 13100(e), in turn, states that "the recording, reporting, storage, analysis, and dissemination of criminal offender information in this state must be made more uniform and efficient, and better controlled and coordinated."[24]

Summary criminal justice information is information pertaining to "the identification and criminal history of any person, such as name, date of birth, physical description, dates of arrest, arresting agencies and booking numbers, charges, dispositions, and similar data about a former criminal offender."[25] Local law enforcement agencies are allowed to freely exchange summary criminal history information (i.e. RAP sheets), provided that the information is a product of the agencies' independent efforts and it is not an investigatory record.

Non-summary information includes information such as intelligence, analytical, or investigative reports and files, or sensitive individual information as it evolves during the stages of prosecution, incarceration, probation, and parole. Non-summary information is defined negatively by the statute: "[L]ocal summary criminal history information does not refer to records and data compiled by criminal justice agencies other than that local agency, nor does it refer to records of complaints to or investigations conducted by, or records of intelligence information or security procedures of, the local agency."[26]

Victims' information is also not included in summary information. The California Constitution contains a Victims' Bill of Rights (VBR), which sets strict prohibitions on the type of information state and county agencies can release about a victim or a victim's family. California voters updated the VBR in 2008 through Proposition 9, introducing several layers of complexity to issues surrounding the release of victim information and the victim's right to refuse discovery requests by the defense. Due to the

---

agencies at all levels of government which perform as their principle functions, activities which either: (a) relate to the apprehension, prosecution, adjudication, incarceration, or correction of criminal offenders; or (b) relate to the collection, storage, dissemination or usage of criminal offender record information." *Id.* § 13101(A)-(B).

[23] *Id.* § 13100(A).

[24] *Id.* § 13100(E).

[25] *Id.* § 13300(A)(1).

[26] CAL. PENAL CODE § 13300(a)(2) (2009).

recent enactment of Proposition 9, courts have yet to offer guidance on how the statute should be interpreted. In the meantime, state and county agencies should establish very clear procedures on how to tag, exclude, or excise this information so that the general public and/or defense does not gain access.[27] The Victims' Bill of Rights is discussed in greater detail *infra* in Part IV.

Generally speaking, disclosure of summary criminal justice information to other criminal justice agencies will expose an agency to no liability, particularly if both have access to CLETS.

A. Disclosure of Summary Information to California Criminal Justice Agencies

Criminal justice agencies in California are required to compile local summary criminal history information. The California Penal Code defines criminal justice agencies as "those agencies at all levels of government which perform as their principle functions, activities which either: (a) relate to the apprehension, prosecution, adjudication, incarceration, or correction of criminal offenders; or (b) relate to the collection, storage, dissemination or usage of criminal offender record information." *Id.* § 13101(A)-(B).

Penal Code Section 13300(1) sets for the requirements for collecting and disseminating selected "local summary criminal history information."[28] A local criminal justice agency must, upon request, share local summary criminal history information with selected parties, including public defenders and attorneys of record, district attorneys, courts, probation officers, and the former criminal offender.[29] And these sections of the Penal Code are intimately tied to Government Code Section 15152 et seq., establishing the CLETS system, because they clarify the data elements to be

---

[27] The VBR creates three sets of issues for criminal justice information sharing, and these issues vary in their relevance and clarity.

First, many provisions of the VBR involve certain "criminal procedure rights" for victims, including the ability to participate in legal proceedings and to confer with prosecutors over the disposition of cases. On the whole, these provisions, though important and controversial, have no bearing on the information issues in this Primer.

Second, the VBR grants victims a right to be informed of certain aspects of the case as it proceeds. This set of rights involves a kind of required information-sharing. Because this information is usually public anyway, the rights simply accelerate disclosure and personal notice.

Finally, and most relevant to this Primer, the VBR sets limits on disclosure of certain categories of information about victims. The bulk of this section deals with those restrictions.

[28] *Id.* § 13300(3)(B)(1)-(16).

[29] *Id.* § 13300(3)(B)(1)-(16).

used in criminal justice databases accessible via CLETS.

The aspect of CLETS most relevant to this Primer is the secondary dissemination of CLETS information. (Agencies regularly share data through joint agreements[30] or under regional arrangements that disseminate data across many different jurisdictions, most notably through Regional Information Sharing Systems (RISS)). The California Department of Justice explicitly allows secondary dissemination of information accessed through CLETS, provided certain regulations are followed.[31] RISS users, who are funded by the federal government, must similarly comply with federal privacy regulations prior to secondary dissemination.[32] These security regulations do not prevent secondary data sharing entirely, but must be incorporated into joint power agreements or contracts with third-party vendors in order to protect privacy and security concerns.

The California Attorney General is "responsible for the security of criminal record information" and is required to enact regulations to protect criminal records from "unauthorized access and disclosure."[33] Information can be shared only when it is "demonstrably required" for "an agency's or official's functions."[34] Secondary dissemination of CLETS information to other law enforcement agencies, including federal agencies, is proper if a "compelling need" is demonstrated and "the information is needed for the performance of their official duties."[35] The California DOJ defines the criterion for release – release occurs "on a need-to-know basis . . . to persons or agencies authorized by court order, statute, or decisional law to receive criminal offender record information."[36] These security

---

[30] MEMORANDUM OF AGREEMENT, *supra* note 2.

[31] DEPT. OF JUSTICE, STATE OF CALIFORNIA, CLETS POLICIES, PRACTICES AND PROCEDURES §1.6.4(J) (Draft Oct. 2008) [hereinafter CLETS PPPs] ("Secondary dissemination and remote access to data accessed via the CLETS using communications media (including the Internet) is allowed when a minimum set of administrative and technical requirements that include the encryption and firewall requirements . . . are met. . . . Any secondary dissemination of the data must be secure and only to those who are authorized to receive the data.").

[32] "Each RISS center must comply with DOJ, BJA Program Guidelines. Information retained in RISS criminal intelligence databases must also comply with the Criminal Intelligence Systems Operating Policies (Federal Regulation 28 CFR Part 23)." Regional Information Sharing Systems, http://www.riss.net/overview.aspx (last visited March 20, 2009).

[33] CAL. PENAL CODE § 11077 (2009).

[34] *Id.*

[35] *See id.* §11105(c)(5).

[36] CAL. CODE REGS. tit. 11, § 703 (2009).

requirements apply not only to the records maintained by the California DOJ, but also to criminal justice records containing CLETS material maintained by any local or state criminal justice agency.[37]

To ensure that agencies conform to applicable security requirements when accessing CLETS data, the California legislature has directed the Attorney General to establish an Advisory Committee to draft CLETS "Policies, Practices and Procedures" (PPPs).[38] The PPPs classify CLETS information as "confidential," and, tracking the regulatory language, limit access to "authorized law enforcement or criminal justice personnel" on a "right-to-know and need-to-know" basis.[39]

B. Disclosure of Summary Information to Criminal Justice Agencies Outside the State of California

Agencies that wish to access CLETS data in the first instance must apply to become subscribers of CLETS and win approval by the Advisory Committee.[40] Because the U.S. Department of Justice and the Federal Bureau of Investigation (FBI) are officially certified subscribers, both agencies are treated like state criminal justice agencies, openly sharing relevant CLETS information for active investigations.[41]

In sum, California officials who are part of CLETS can be confident that any secondary dissemination of CLETS information to another state or

---

[37] Criminal Record Information is defined as "records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release." CAL PENAL CODE §11075

[38] CAL. GOV'T CODE §§ 15154, 15160 (2009).

[39] CLETS PPPS, *supra* note 31, at § 1.6.4.

[40] *Id.* at §1.3 (listing the FBI as a Class I authorized subscriber, and also listing non-law enforcement personnel under Class II and III levels).

[41] Even when local authorities share non-CLETS information with federal authorities for law enforcement purposes, including information from Records Management Systems or Computer Aided Dispatch, there is little danger of being sued for invasion of privacy. If the information is public record, for instance, the disclosure would be controlled by the CPRA, discussed in Part III. If a federal agent uses the information illegally, that agent, not the local authority, would be responsible for the illegal activity. There are few other legal remedies for alleged privacy violations as a result of disclosure. *See, e.g.*, Hilary Hylton, *Fusion Centers: Giving Cops Too Much Information*, TIME, Mar. 9, 2009, http://www.time.com/time/nation/article/0,8599,1883101,00.html.

federal law enforcement agency for a legitimate law enforcement purpose will not create legal liability, so long as they comply with CLETS security rules, discussed in Section C *infra*. Those rules are somewhat technical and complex, especially those concerning who is a subscriber agency and when information can be released to a non-subscriber agency with a need to know related to law enforcement. The key to compliance is for all officials with power over CLETS information to be familiar with the rules in the latest CLETS PPPs. That document contains a user-friendly guide to the rules, along with sample forms for situations like the release of information to non-subscribers.

C. Disclosure of Summary Information to California Agencies that are not part of the Criminal Justice System

Once an agency, federal or local, has access to CLETS, it must comply with the confidentiality policies and technical security requirements of the PPPs. Agencies cannot access or secondarily release CLETS information "for non-law enforcement purposes . . . unless otherwise mandated," and, if they do, they are "subject to administrative action and/or criminal prosecution."[42] Secondary dissemination of CLETS data, particularly through regional or interagency sharing arrangements, moreover, must comply with electronic security requirements, including "encryption and firewall" protections. Secondary dissemination specifically requires that CLETS information be released only to "those who are [otherwise] authorized to receive the data," specifically an agency that is a valid law-enforcement organization with a need-to-know or right-to-know.[43] This limitation generally prevents local police departments from sharing CLETS derived information with organizations like local health providers or human service agencies, which are not law enforcement agencies with a right to access CLETS data directly.

III. MEDICAL INFORMATION: INFORMATION SHARING AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

[42] CLETS PPPs, *supra* note 31, at §§ 1.6.4; 1.10; *see also* CAL. PENAL CODE §§ 11141-11144 (2009) (explaining that Department of Justice employees who give (or receive) criminal history information to unauthorized parties is guilty of a misdemeanor); *Id.* § 13302 (2009) (local criminal justice agency employees are guilty of misdemeanor when furnish a criminal record to unauthorized individual). Officials, however, would have a defense if the transfer of information were necessary for the apprehension of a person suspected of a crime. *Id.* § 13304(c).

[43] CLETS PPPS, *supra* note 31, at § 1.6.4.

Criminal justice agencies want information about the health needs of people under their care or supervision. The issue in this section deals primarily with health care providers' reported reluctance to share medical information out of the belief that it will compromise patient privacy under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA "Privacy Rule," which took effect in 2001, regulates the use and disclosure of health information held by covered entities.[44] Generally, HIPAA requires an individual's valid authorization to reveal the individual's "Protected Health Information," which is broadly defined to include any information concerning the person's health status, provision of medical care, or payment for care that can in any way be identified to him or her.[45] One component of HIPAA deals with individuals' entitlement to get their own medical information from covered entities. Another confirms that individuals can consent to or authorize disclosure of medical information to third parties, although even then the covered entity is required to limit any such disclosure to the minimum necessary to accomplish the intended purpose motivating the person's permission.[46] Of key relevance to this Primer are HIPAA's provisions that permit disclosure to third parties without the individual's permission.[47]

Many officials are generally aware of HIPAA and understandably worry that it may constrain their use of information about individual records, but these concerns are largely unfounded. These default rules are punctuated with an array of exceptions that make HIPAA "a maze of intertwined and interlocking puzzle pieces"[48] but the ultimate inference to be drawn from this legal maze is fairly straightforward: HIPAA rarely poses challenges to officials in criminal justice agencies if they use medical information for any conventional criminal justice purpose.

HIPAA only directly applies to "covered entities." These include

---

[44] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH INFORMATION PRIVACY: SUMMARY OF THE HIPAA PRIVACY RULE (2009), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Apr. 16, 2009).

[45] 45 C.F.R. § 164.508(a)(1) (2009).

[46] 45 C.F.R. § 164.502(b) (2009).

[47] Such disclosure is often described as "unauthorized" disclosure, although that term is confusing. It is not authorized by the individual but may be authorized by statute or regulation.

[48] Tamela J. White & Charlotte A. Hoffman, *The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos.* 106 W. VA. L. REV. 709, 712 (2004).

(1) health plans (such as health insurance companies or Medicaid), (2) health care clearinghouses (entities that process nonstandard health information, such as billing companies that convert information into data content); and (3) health care providers (such as hospitals and doctors).[49] Thus, justice agencies like courts and law enforcement agencies will rarely *generate* the information that is protected by the HIPAA privacy rule. Normally, the only "covered entities" within the justice system will be prisons or jails directly providing health care. In such cases, the medical personnel in the place of incarceration need to be aware of HIPAA, just as if they were working in civilian hospitals or clinics, and their non-medical supervisors will have to ensure that the medical personnel remain in compliance.

HIPAA, as a result, mainly affects criminal justice agencies in their role as potential *receivers* of medical information from covered entities: health care providers might be reluctant to release information to governmental agencies because those providers fear liability under HIPAA. The key concern in this section is how covered providers can be assured that justice agencies who receive information are complying with HIPAA in their inter-agency information sharing and therefore do not expose the entities to liability.

A. HIPAA Liability for Covered Entities

Despite the concerns of health care providers, HIPAA penalties have rarely been imposed. Criminal justice agencies seeking health care information must nevertheless expect covered entities to be risk-averse to extensive information disclosure and potential liability. The criminal justice agencies must, as a result, be conversant with the rules and exceptions in HIPAA to assure providers that they will not risk liability by improperly transferring information.

Illustrative civil penalties for a single HIPAA violation by an institution (referred to as a violation of an "identical requirement or prohibition") can be up to $25,000 a year.[50] Depending on how narrowly the phrase "identical requirement or prohibition" is construed, the maximum annual penalty could be many times more than $25,000.[51]

---

[49] 45 C.F.R. § 160.103 (2009).

[50] 42 U.S.C. § 1320d-5 (2000).

[51] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH INFORMATION PRIVACY: CASE EXAMPLES AND RESOLUTION AGREEMENTS (2009), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

HIPAA also includes penalties for individuals who violate the statute, including a $50,000 fine and up to one year in prison for a knowing violation, and a $250,000 fine and up to ten years in prison for a violation for financial gain.[52]

Despite these statutory penalties, HIPAA is rarely enforced.[53] Violations are not enforced in court because the statute contains no private right of action.[54] In fact, an individual's only response to a perceived HIPAA violation is to file a complaint with the Department of Health and Human Services (HHS).[55] In the past, HHS has been extremely reluctant to impose penalties – not one of the thousands of complaints filed before 2008 resulted in a single penalty being imposed.[56] As of March 31, 2009, HHS has received over 43,052 HIPAA privacy complaints. HHS has dismissed the vast majority of these cases and resolved the others by requiring entities to implement new policies.[57] HHS has imposed sanctions a mere two times.[58]

(last visited Apr. 16, 2009) (referring to case where sanctions are imposed as "resolution agreements").

[52] 42 U.S.C. § 1320d-6(b) (2000).

[53] Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672.html

[54] Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006); *see also* 45 CFR § 160.306(a) (2009).

[55] 45 C.F.R. § 160.306(a) (2009).

[56] JOHN PETRILA, NAT'L GAINS CTR., DISPELLING MYTHS ABOUT INFORMATION SHARING BETWEEN THE MENTAL HEALTH AND CRIMINAL JUSTICE SYSTEMS 4 (2007); *see also* Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 202 n.15 (2007).

[57] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH INFORMATION PRIVACY: ENFORCEMENT HIGHLIGHTS (2009), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html (last visited Apr. 16, 2009).

[58] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, *supra* note 212 (referring to case where sanctions are imposed as "resolution agreements"). Criminal sanctions have been similarly sparse. As of March, 2009, there have been eight criminal convictions under HIPAA; in each case, the convicted individual used private medical information for personal financial gain. *See* Rebecca Herold, *HIPAA Criminal Convictions Outpace Sanctions*, SEARCHCOMPLIANCE.COM, Mar. 23, 2009, http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1351658,00.html.

Despite the rarity of sanctions, government agencies might face significant challenges when seeking information from health care providers. HHS has the power to change its tactics any time. In fact, there are some signs that enforcement is rising: both instances of sanctions were recent (July 16th, 2008 and January 16th, 2009).[59] Even more troubling, the sanctions were significant ($100,000 for failing to safeguard information against theft and loss, and a $2.25 million against CVS for failing to dispose properly of protected health information and for failing to sanction employees who violated HIPAA). In the approximately 8,000 other cases not dismissed for lack of merit, however, HHS has simply directed providers to change their policies.[60]

Criminal justice agencies can utilize several arguments to reassure health care entities reluctant to produce information. Even if the HHS accelerates enforcement, it is highly unlikely that it would impose penalties on entities collaborating with governmental agencies in good faith, particularly those in the criminal justice system.[61] But the best assurance that a criminal justice agency can give a health care provider is that that the request is explicitly permissible under HIPAA. The key, therefore, is that criminal justice agencies understand the HIPAA exceptions.

B. HIPAA Exceptions

HIPAA presumptively requires an individual's valid authorization to

---

[59] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, *supra* note 212 (referring to case where sanctions are imposed as "resolution agreements").

[60] *Id.*; UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, *supra* note 219.

[61] UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH INFORMATION PRIVACY: SUMMARY OF THE HIPAA PRIVACY RULE (2009), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Apr. 16, 2009) ("Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make."); UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, HEALTH INFORMATION PRIVACY: ALL CASE EXAMPLES (2009), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case17 (last visited Apr. 16, 2009).

In this case, a chain pharmacy violated HIPAA in impermissible uses and disclosures to law enforcement officials. OCR directed the chain to revise its policy, revealing information "only in response to written requests from law enforcement officials."

reveal that individual's health information [62] and, as noted, the covered entity must also limit any information it discloses to the minimum necessary to accomplish the purpose intended by the individual.[63] But exceptions to HIPAA delineate a subset of information that may be released without authorization in particular circumstances; those relevant here are disclosures:

1. To a correctional institution and other law enforcement custodial situations;[64]
2. For treatment purposes;[65]
3. To the extent that disclosure is required by law;[66]
4. About victims of abuse, neglect or domestic violence;[67]
5. For judicial and administrative proceedings;[68]
6. To avert a serious threat to health or safety;[69]
7. For law enforcement purposes.[70]

As discussed more below, HIPAA will sometimes permit disclosure if a particular state law mandates it. This principle raises an unusual inconsistency under HIPAA. On the one hand, the HIPAA exceptions do not allow the disclosure of notes taken during a private counseling session, which always require authorization.[71] On the other hand, California's *Tarasoff* principle *requires* a psychotherapist to disclose information from a private counseling conversation when the client poses a potential danger to others.[72] This requirement, in turn, triggers HIPAA's exception for a use or disclosure that is required by law, meaning that the notes can be disclosed without fear of HIPAA sanctions.[73] (This particular example would also trigger the HIPAA exception for avoiding a threat to public safety,

---

[62] 45 C.F.R. § 164.508(a)(1) (2009).
[63] *Id.* § 164.502(b).
[64] *Id.* § 164.512(k)(5).
[65] *Id.* § 164.502(a)(1)(ii).
[66] *Id.* § 164.512(a).
[67] *Id.* § 164.512(c).
[68] *Id.* § 164.512(e).
[69] *Id.* § 164.512(j).
[70] *Id.* § 164.512(f).
[71] *Id.* § 164.508(2).
[72] Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 347 (Cal. 1976) ("[T]he public policy favoring protection of the confidential character of patient-psychotherapist communications must yield to the extent to which disclosure is essential to avert danger to others. The protective privilege ends where the public peril begins.").
[73] 45 C.F.R. § 164.512(a)(1) (2009).

discussed *infra* at 23.)

Key aspects of the HIPAA exceptions include:

1. A Custodial Situation

A covered entity may disclose protected health information to a correctional institution or a law enforcement official who has lawful custody over an individual.[74] When an individual ceases to be in lawful custody (for instance, when he begins parole or supervised release), these provisions no longer apply.[75] While the individual is in custody, disclosure may be made only insofar as necessary for:

1. Providing health care to the individual;

2. The health and safety of the individual, other inmates, employees, or others at the correctional institution;

3. The health and safety of those transporting the individual;

4. Law enforcement on premises of a correctional institution, or the maintenance of safety, security and good order of the correctional institution.[76]

This exception will encompass a wide array of desired uses of medical information. But it only applies while the individual is in custody; it will not reach individuals who are on community supervision, and it focuses on treatment or general safety purposes, not law enforcement broadly defined. Moreover, it is unclear whether dealing with an individual's drug or mental health problems will always qualify as treatment or as necessary for safety. Nevertheless, even this limited exception will encompass many desired uses, and citing this exception can be effective in reassuring reluctant covered entities to release information.

2. For Treatment Purposes

Unauthorized disclosure is permitted "for treatment activities of a health care provider."[77] The regulations do not stipulate who qualifies as a

[74] *Id.* § 164.512(k)(5)(i).
[75] *Id.* § 164.512(k)(5)(iii).
[76] *Id.* § 164.512(k)(5)(i).
[77] *Id.* § 154.506(c)(2).

health care provider. They do specify that "[a] covered entity may disclose protected health information to another covered entity *or* a health care provider for the payment activities"[78] (emphasis added). Thus, the regulations seem to contemplate a health care provider who is not a covered entity. If a health care provider is broadly defined, many aspects of criminal justice information sharing could fall into this exception. It is possible that even a police officer acting as a treatment facilitator could qualify as "a health care provider" who is not a covered entity. In the absence of case law interpreting this language, however, it is unclear whether the regulations intend this broad reading.

3. Disclosure Required by Law

A covered entity may use or disclose protected information to the extent that such use or disclosure is required by another law.[79] In disclosing the information required by another law, "the covered entity must simply comply with the requirements of the other law."[80] This is a broad exception; "law" includes "the full array of binding legal authority, such as constitutions, statutes, rules, regulations. . . . It encompasses federal, state or local actions with legally binding effect."[81]

This exception would facilitate receiving information from outside agencies whenever a law requires disclosure. Thus, if California passes a law *requiring* disclosure of medical information, for instance in response to a written request by a governmental agency, virtually all legal hurdles would be eliminated. This requirement would satisfy HIPAA. It would, as discussed below, also satisfy requirements of the Confidential Medical Information Act (CMIA). The only limitation requires that the use be reasonable so as not to violate the right to privacy under the California Constitution.[82]

4. Victims of Abuse, Neglect, or Domestic Violence

Information about victims of abuse, neglect, or domestic violence may be disclosed only when disclosure is expressly authorized by law. The

---

[78] *Id.*

[79] *Id.* § 164.512(a)(1).

[80] Prot. & Advocacy Sys., Inc. v. Freudenthal, 412 F. Supp. 2d 1211, 1218 (D. Wyo. 2006) (citing Ohio Legal Rights Serv. v. Buckeye Ranch, Inc., 365 F. Supp. 2d 877, 886 (S.D. Ohio 2005)).

[81] *Id.*

[82] *See* note 286, *infra*, and accompanying text.

victim, moreover, must be unable to agree to the disclosure because of incapacity. Disclosure may also be justified if it is necessary to prevent serious harm to the victim or other potential victims.[83]

5. For Judicial and Administrative Proceedings

In the course of a judicial or administrative proceeding, a covered entity may disclose protected information expressly authorized by a court order.[84] It may also reveal information in response to a subpoena, discovery request, or "other lawful process."[85] In this case, California law requires that the requesting party serve a Consumer Notice to the individual whose records are being sought before those records can be disclosed.[86] As discussed below, having judges issue standing court orders mandating the sharing of relevant information is a possible way to avoid HIPAA concerns. This is a particularly useful tool because, under California law, entities are *required* rather than simply permitted to disclose information pursuant to a court order.[87] Thus, if a county has a standing court order that medical records of arrested individuals be released to the arresting officer, a health care provider will be required, rather than simply permitted, to disclose the medical record.

Note that these exceptions establish that even when HIPAA operates as a *confidentiality* law—i.e., limiting out-of-court disclosure—it does not serve as an evidentiary privilege law (see, *supra,* Part VI. C.). That is, the covered entity does not have any privilege to resist providing evidence or testimony in a formal legal proceedings.

6. To Avoid a Serious Threat to Health and Safety

A covered entity may also reveal health information necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or to the public.[88] This includes identifying or apprehending an individual who "appears from all circumstances" to have escaped from a correctional institution or other lawful custody.[89] It may also be used to identify an individual who confessed to participating in a violent crime,

---

[83] 45 C.F.R. § 164.512(c) (2009).
[84] *Id.* § 164.512(e)(i).
[85] *Id.* § 164.512(e)(ii).
[86] CAL. CIV. PROC. CODE § 1985.3 (2005).
[87] CAL. CIV. CODE § 56.10(b) (2009).
[88] 45 C.F.R. § 164.512(j) (2009).
[89] *Id. § 164.512(j)(1)(ii)(B).*

unless the confession was made through a request by the individual to receive counseling[90] or during treatment to reduce the propensity to commit such a crime.[91] The release must be made to a person able to prevent or lessen the threat, such as a police officer or the target of the threat.[92] The releasable information is limited to the statement itself, and identifying information such as the individual's name and physical appearance.[93]

7. Law Enforcement Purposes

Under certain circumstances, a covered entity "may disclose health information for a law enforcement purpose to a law enforcement official."[94] Besides circumstances that fall into one of the previously addressed exceptions, disclosure is also permitted, subject to the Victims' Bill of Rights, when:

1. The individual is suspected of being the victim of a crime, and the covered entity is unable to obtain permission to release from the individual. Further, the information must be necessary to investigate the crime;[95] or

2. The individual is dead, and the covered entity has a suspicion that such death may have resulted from criminal conduct;[96] or

3. The information is evidence of criminal conduct that occurred on the premises of the covered entity;[97] or

4. There is a medical emergency, not on the premises of the covered entity, and release of the information is necessary to report the nature or location of a crime, or the identities of those involved in a crime.[98]

C. Policy Suggestions for Information Sharing Under HIPAA

---

[90] *Id. § 164.512(j)(2)(ii).*
[91] *Id.* § 164.512(j)(2)(i).
[92] *Id.* § 164.512(j)(1)(i)(B).
[93] *Id.* § 164.512(j)(3).
[94] *Id.* § 164.512(f).
[95] *Id.* § 164.512(f)(3)(ii).
[96] *Id.* § 164.512(f)(4).
[97] *Id.* § 164.512(f)(5).
[98] *Id.* § 164.512(f)(6).

Because there is always the threat of sanctions, even "toothless"[99] HIPAA provisions can interfere with information sharing. Where information does not clearly fall into one of the HIPAA exceptions, or where only some of the information falls into an exception, several options remain.

- HHS Advisory Opinion: The best solution is for the HHS to issue an advisory opinion that HIPAA will not be enforced against criminal justice information sharing. The HHS could posit that such sharing would fall within HIPAA, that it will simply not enforce HIPAA provisions against entities responding to governmental requests for information, or even that it will limit any interference to policy recommendation rather than sanctions.

- State or Local Law Requiring Disclosure: California could pass a law (or several local laws can be passed) requiring disclosure to governmental agencies.

- Uniform Consent Forms:[100] An individual entering the criminal justice system could sign a form listing all relevant entities who can receive the information (e.g. parole officers, police officers, prison officials), thus obtaining the individual's consent for each entity on the list. An individual could either check a box next to each entity or could sign a statement that he authorizes disclosure to 'all the entities listed above.'

- Judicial Order: Another option used in some jurisdictions is for judges to create judicial orders with standard language mandating the sharing of information with relevant entities.[101] To comply with California law, a Consumer Notice would have to be delivered to the individual before records are disclosed.[102]

- Case-by-case Clarification for Outside Agencies: Before one of the above approaches takes effect, criminal justice agencies could persuade outside agencies to share information by citing the low enforceability of HIPAA or a relevant exception that makes the disclosure permissible.

---

[99] Collins, *supra* note 58, at 199.
[100] PETRILA, *supra* note 58, at 3.
[101] *Id.*
[102] CAL. CIV. PROC. CODE. § 1985.3 (2005).

D. State Law and the Confidential Medical Information Act (CMIA)

Because the enforceability of HIPAA has been limited, many of the problems of information sharing might, instead, arise directly under relevant state law. California's version of HIPAA is the Confidentiality of Medical Information Act (CMIA). Under CMIA, a patient who is harmed through unlawful disclosure can receive monetary damages. CMIA provides that violations are misdemeanors;[103] it entitles the patient to compensatory damages, up to $3,000 in punitive damages, up to $1,000 in attorney's fees, and litigation costs.[104]

A key question is when HIPAA preempts provisions of state law. In the abstract, federal law, under the Supremacy Clause, preempts state law whenever the two are contradictory. But that abstract principle is very difficult to apply in specific instances, because whether two laws are contradictory or mutually inconsistent cannot always be derived from statutory language; it requires reference to the statutes' manifest purposes and operations.

Like some other complex federal laws, the HIPAA Privacy rules contain their own preemption rules. They look dauntingly complex themselves, but their implications are fairly clear.

The best way to imagine the preemption rule is as follows: since HIPAA's purpose is to guide officials of covered entities in regard to disclosure, first one asks whether a state official faces any contradiction in complying with both HIPAA and the state law in question. If doing something she is permitted or required to do under state law would require her to simultaneously violate HIPAA, then federal law nullifies the state law. Thus, in general terms, if a state law permits or requires a disclosure of protected medical information where HIPAA bars it, then the official must comply with the HIPAA bar.

HIPAA, nevertheless, contains provisions whereby an apparent preemption is overcome. For example, when a state rule appears preempted, the Secretary of HHS can still defer to the state law. In such situations, it is necessary that the Secretary seek to prevent abuse in health care or regulation of health insurance, and that there be a compelling public

---

[103] CAL. CIV. CODE § 56.36 (2009).
[104] *Id.*

safety justification as balanced against privacy (unless the state law is more stringent in its protections).

Thus, HIPAA preempts a contrary state law only insofar as the state law provision is less stringent than HIPAA.[105] The more restrictive provision between HIPAA and state law will consequently govern. HIPAA provisions are more restrictive in a majority of cases. A few particularly relevant distinctions between HIPAA and CMIA are:

- CMIA allows broad disclosure for medical purposes, including disclosure to health care providers, service plans, contractors, and "other health care professionals or facilities," and permits disclosure for diagnosis as well as treatment.[106] This exception is more likely to encompass activities of criminal justice agents than HIPAA, which allows disclosure only for treatment and only to a health care provider.[107] HIPAA would thus apply.

- A section of CMIA added in 2007 allows disclosure of medical information to a county social worker, a probation officer, or any other person legally authorized to have custody or care of a minor for purposes of coordinating health care services and medical treatment for the minor.[108] HIPAA does not specifically address parole officers, but allows disclosure to anyone acting "in loco parentis," unless the only consent required is the consent of the unanticipated minor.[109] HIPAA would thus apply.

- CMIA *requires*, rather than simply permits disclosure pursuant to a court order or a search warrant.[110] CMIA would thus apply.

HIPAA provisions are the more restrictive in a majority of cases, but—likely due to the lack of a private right of action and general low enforceability of HIPAA—California cases about disclosure of medical information consider only state law.[111] In a 2006 case, for instance, the

---

[105] 45 C.F.R. § 160.203(b) (2009).
[106] CAL. CIV. CODE § 56.10(c)(1) (2009).
[107] 45 C.F.R. § 154.506(c)(2) (2009).
[108] CAL. CIV. CODE § 56.103 (2009).
[109] 45 C.F.R. 164.502(g)(1)(3) (2009).
[110] CAL. CIV. CODE § 56.10(b) (2009).
[111] *See, e.g.*, Cal. Consumer Health Care Council v. Kaiser Found. Health Plan, Inc., 47 Cal. Rptr. 3d 593, 597 (Ct. App. 2006) (ruling based on exception in

court held that release of medical information to attorneys was authorized by CMIA despite plaintiffs' claim that some of the information was irrelevant. The court held that "the Legislature specifically elected not to graft a relevancy limitation onto the section 56.10(c)(4) exception." However, an exception without a relevancy limitation is preempted by HIPAA's more stringent "minimum necessary" requirement. Technically, HIPAA governed and the plaintiffs should have prevailed. Yet the court did not address the issue, nor did the decision mention HIPAA.[112]

Insofar as California law governs even where HIPAA would be more stringent, CMIA offers a simple solution. It holds that "information may be disclosed when the disclosure is otherwise specifically authorized by law, including, but not limited to, the voluntary reporting" to the FDA.[113] This exception applies whenever a law indicates that disclosure should occur. Courts have interpreted the "authorized by law" exception very broadly. In *Shaddox v. Bertani*, a dentist reported his suspicions that a police officer patient had a prescription drug problem to the officer's superiors.[114] The court held that the dentist's actions were lawful because city charter provisions encouraged reporting of complaints of police misconduct. This qualified as "specifically authorized," although the provisions did not mention medical information. *Shaddox* also indicates that CMIA governs: it explicitly acknowledged HIPAA,[115] but decided the case solely by reference to CMIA.[116]

The best option to satisfy CMIA would be to pass a law at the city, county, or state level that authorizes disclosure of medical information. Under *Shaddox*, this law could simply be a statement that the State of California encourages criminal justice information sharing. A legal authorization

---

CMIA, although the CMIA exception would be preempted by HIPAA's minimum necessary standard); Colleen M. v. Fertility & Surgical Assoc. of Thousand Oaks (2005) 34 Cal. Rptr. 3d 439, 443 (Ct. App. 2005) (.holding that a clinic's disclosure of medical information to ex-fiancé was authorized under CMIA 56.10(c)(2) when the patient used ex-fiancé's credit card to pay at health clinic, even though the disclosure technically violated HIPAA's requirement that payment information be released only to a health care provider or other covered entity (45 C.F.R. § 154.506(c)(2)).

[112] *Cal. Consumer Health Care*, 47 Cal. Rptr. 3d at 597.

[113] CAL. CIV. CODE § 56.10(c)(12) (2009).

[114] Shaddox v. Bertani, 2 Cal. Rptr. 3d 808, 817 (Ct. App. 2003).

[115] *Id.* (mentioning the passage of HIPAA as an example of "concerns about medical privacy").

[116] *Id.* at 814-15.

would trigger the 56.10(c)(4) exception. Though it wouldn't satisfy HIPAA, California case law indicates that HIPAA does not normally come into play in California cases. Moreover, an explicit authorization at the state level would make any adverse action by the HHS under HIPAA even more unlikely.

IV. VICTIMS' ISSUES

The California Victims' Bill of Rights (VBR) changes the information exchange landscape in two ways. First, it grants crime victims the right to access summary information. Second, it limits the disclosure of information about victims. Each will be discussed in turn.

A. Disclosure of Summary Information to Victims

Proposition 8 (the Victims' Bill of Rights) was passed in 1982 and amended the California Constitution. It also enacted several statutes, including those concerned with the rights victims to be notified in advance of sentencing and parole hearings, as well as to participate in and offer a victim statement in these hearings.[117] Proposition 9 (Victims' Rights and Protection Act), more commonly known as Marsy's Law, was approved in 2008 with the goal of broadening victims' rights and making them more enforceable. The 2008 law provides a basic definition of what it means to be a victim under the law,[118] and, through Penal Code Section 679.026(b), provides that a victim has the right to receive, without cost or charge, a complete list of the rights recognized in Section 28 of Article I of the California Constitution.[119] The various rights established by Proposition 9

[117] Most notably, Proposition 8 added Section 28 to Article 1 of the Constitution and created Penal Code Section 1191.1, which established the right of crime victims to obtain restitution from the perpetrator.

[118] CAL. CONST. art. 1, § 28(b)(17)(e) (2008).

[119] Proposition 9 is not a standalone provision for victims' rights. It is designed to be a part of a cohesive framework of victims' rights. Proposition 9 Initiative Measure § 7 (Conflicts with Existing Law) states the following: "It is the intent of the People of the State of California in enacting this act that if any provision in this act conflicts with an existing provision of law which provides for greater rights of victims of crimes, the latter provision shall apply." CA PROP. 9 (2008). *See also* CAL. PENAL CODE SECTION 13835(A)-(F) (2008) ("[T]here is a need to develop methods to reduce the trauma and insensitive treatment that victims and witnesses may experience in the wake of a crime, since all too often citizens who become involved with the criminal justice system, either as victims or witnesses to crime, are further victimized by that system. . . . It is, therefore, the intent of the Legislature to provide services to meet the needs of both victims and witnesses of

are constitutionally protected and enforceable in any trial or appellate court.[120]

In general, Proposition 9 expanded the notification and participation rights of victims in criminal justice proceedings previously mandated by Proposition 8.[121] Under Proposition 9, victims must be notified of all criminal proceedings including pretrial proceedings and the transfer or release of defendants, whereas Proposition 8 only required criminal justice agencies to notify victims about upcoming sentencing and parole hearings. Prosecutors are now required to take reasonable steps to confer with crime victims about its charging decisions and developments related to the filing of charges.[122] These participatory and conferral rights are important, and they have created controversy over whether they unduly impinge on the prosecutor's prerogative.[123] Nevertheless, they do not, by themselves, raise

---

crime through the funding of local comprehensive centers for victim and witness assistance.").

[120] CAL. CONST. art. I, § 28(C)(1) (2008) ("A victim, the retained attorney of a victim, a lawful representative of the victim, or the prosecuting attorney upon request of the victim, may enforce the above rights in any trial or appellate court with jurisdiction over the case as a matter of right. The court shall act promptly on such request.").

[121] *See generally*, Harriet Salarno, *Prop. 9 Expands Crime Victim's Rights*, SF CHRONICLE, Oct. 9, 2008, at B7; LEGISLATIVE ANALYST'S OFFICE, HEARING HANDOUT, PROPOSITION 9: VICTIM'S BILL OF RIGHTS ACT OF 2008: MARSY'S LAW (Sept. 23, 2008) (presented to the Assembly and Senate Public Safety Committees), *available at* http://www.lao.ca.gov/LAOApp/PubDetails.aspx?id=1885 (last visited on Mar. 18, 2009).

[122] CAL. CONST. art. 1, § 28(b)(6) (2008).

[123] It is unclear whether the new conferral rights afforded to victims will impinge on a prosecutor's objectivity and independence. A victim's right to "reasonably confer" with the prosecution is somewhat ambiguous: Does it mean that a prosecutor is simply required to ask for input from the victim? Is the prosecutor required to do more than keep an open line of communication with a victim? The chief concern regarding the conferral rights created under Article 1, Section 28(b)(6) of the Constitution is that prosecutors have more nuanced understandings of criminal proceedings and may face increasing pressure from a victim to adopt a certain course (i.e., what charges should be in an indictment). Even if a victim is knowledgeable about the legal and practical obligations that shape a prosecutor's duties and the victim understands the procedural minutia of the criminal justice system, a victim may lack an objective outlook. Consequently, a victim may not make prudent requests for prosecutorial action and may unjustifiably expect more deference in opinion from a prosecutor. Although Article 1, Section 28(b)(6) of the Constitution formalized conferral rights, a

issues related to confidential information.

When Article 1, Section 28(b)(6) of the Constitution is read in conjunction with Article 1, Section 28(b)(7) and Article 1, Section 28(b)(8) of the Constitution, the victim essentially has full access to material dispositional information about the offender.[124] Proposition 9 did not eliminate any of the pre-existing victims' rights to access offender information. Instead, Proposition 9 augmented many of the pre-existing rights that afforded access. As a result, victims can obtain information about an offender either formally (information provided directly to the victim by a representative of a criminal justice agency) or informally (information gained firsthand through attendance at a criminal proceeding in which the victim elects to participate).[125]

Since most of the information about offenders is already available in conventional data sharing networks, an integrated criminal justice system would not improve the quality of victims' rights. An integrated criminal justice system may, however, make existing information sharing networks more comprehensive and thereby facilitate the process of communicating relevant information to the parties responsible for keeping victims duly informed of an offender's status. Another major concern about the expanded victims' notification and participation rights is the costs that the various state and local agencies will bear. Providing information and allowing victims to participate in all criminal proceedings will be costly.[126]

---

prosecutor is not thrust in a new or unfamiliar position of managing a victim's participation. An experienced and competent prosecutor is likely to be adept at managing the interests and concerns of a victim, and likely conferred with victims in the absence of Proposition 9. The prosecutor, however, may encounter difficulties in the form of a victim now believing that a right to confer with the prosecution means he or she has a right to act as a back-seat prosecutor (i.e., unofficial co-counsel).

[124] CAL. CONST. art. 1, § 28(b)(7) (2008); *id.* § 28(b)(8).

[125] Victims' rights to offender information or rights to participate in criminal proceedings are discussed in the several statutory provisions. *See*, *e.g.*, CAL. GOV'T CODE § 6254(f); CAL. PENAL CODE § 679.02(a)(2); *id.* § 679.02(a)(3); *id.* § 679.02(a)(4); *id.* § 679.02(a)(5); *id.* § 679.02(a)(6); *id.* § 679.02(a)(11); *id.* § 679.02(a)(12); *id.* § 679.02(a)(12)(A); *id.* § 679.02(a)(13); *id.* § 679.02(a)(14); *id.* § 680(c)(2)(C); *id.* § 1102.6; *id.* § 1191.1; *id.* § 1202.1(d)(1); *id.* § 1203.05(a)-(c); *id.* § 3043(a)(1); *id.* § 3043(b)(1); *id.* § 3058.8(a); *id.* § 3605(a); *id.* § 11116.10(a); CAL. WELF. & INST. CODE § 656.2(a)-(c); *id.* § 676.5.

[126] *See*, *e.g.*, LEGISLATIVE ANALYST'S OFFICE, HEARING HANDOUT, *supra* note 122.

B. Restrictions on the Disclosure of Information about Victims

Data contained in case management systems might contain information about victims. After the VBR, agencies will need to ensure that confidential information is not released to the defendant in such a way that it exposes the victim to potential harassment. As amended by Proposition 9, the VBR now protects the victim's right:

> 4. To prevent the disclosure of confidential information or records to the defendant, the defendant's attorney, or any other person acting on behalf of the defendant, which could be used to locate or harass the victim or the victim's family or which disclose confidential communications made in the course of medical or counseling treatment, or which are otherwise privileged or confidential by law.
>
> 5. To refuse an interview, deposition, or discovery request by the defendant, the defendant's attorney, or any other person acting on behalf of the defendant, and to set reasonable conditions on the conduct of any such interview to which the victim consents.[127]

The distinction between these two guarantees is important.

Right Four is a broad restriction on the power of government officials to disclose information about the victim where that disclosure meets the criteria of potential harm to the victim.

Right Five limits the duty of the victim herself to disclose information to a criminal defendant. The significance of the latter rule is deceptive until one sets the context. As a general matter, no victim, or any other potential witness to a criminal case is obligated to answer any questions posed by the defendant or the defense team—or even to law enforcement. Rather, the obligation to provide information only arises under some sort of court order or subpoena, as where the victim or witness is called to testify in a preliminary examination, grand jury hearing, or actual trial. Thus, in a sense, Right Five has a symbolic redundancy. On the other hand, if Right Five is meant to restrict the obligation of the victim to provide information even when summoned to testify, then it operates as an evidentiary privilege. This question is explored in more detail below.

---

[127] CAL. CONST. art. 1, § 28(b) (2008).

In light of Right Four, state and county agencies may not release any of the following information to the public, the defendant, the defendant's attorney, or to anyone else acting on behalf of the defendant:

- The victim or the victim's family members' addresses, phone numbers, email addresses, or any other information that could be used to locate or harass the victim or victim's family members

- Confidential information from medical or counseling treatment provided to the victim, including the victim's mental health record

Before the passage of Proposition 9, defendants could request access to a victim's confidential information, such as mental health records or criminal history, and the court could grant the defendant's discovery request if it deemed the information relevant. The 2008 amendments to the VBR revoke the defendant's right to obtain such mental health or criminal history information.

Right Five enables the victim to refuse an interview or deposition request by the defense. Should the victim decide to consent to interviews, he may set reasonable conditions about how those interviews will be conducted. The victim may also refuse a discovery request by the defense. The defense cannot force the victim to turn over any documents, including the victim's criminal history.

In light of these discovery limitations, prosecutors face conflicting obligations. As discussed below in Part VI, prosecutors cannot suppress material exculpatory information (the *Brady* requirement). The VBR, however, suggests that victims can refuse discovery requests, even requests for exculpatory information. Because the VBR is part of the California's Constitution, it arguably trumps discovery rules in both the Penal Code and California Supreme Court decisions. And because the VBR applies to state court proceedings on issues of state law, the prosecutor would normally be bound to follow the VBR over federal law. *Brady* requirements, however, are elements of the United States Constitution and cannot be ignored. Prosecutors, consequently, *must* disclose material exculpatory information. The conflicts between *Brady* and the VBR require careful evaluation of both discovery requests and the applicable evidence to ensure compliance, to the extent possible, with both laws.

V. DISCLOSURE TO PRIVATE PARTIES UNDER SUNSHINE STATUTES

This section deals with disclosure to private parties—that is, non-governmental agencies or individuals. Such disclosure may be mandated under "sunshine" statutes which promote access to government records, such as the California Public Records Act (CPRA) or the federal Freedom of Information Act (FOIA). Again, the framework used will be when the information must be disclosed, when it may be disclosed, and when it may not be disclosed. Generally, all public records must be disclosed under the CPRA, which can include some criminal justice information. The majority of this section will be devoted to a discussion of the CPRA in Part A, with a brief discussion of federal statutes in Part B.

A. The CPRA

A key question for criminal justice officials is whether they are required to guarantee public access to information on the ground that the information constitutes a "public record." The relevant legal rules on this subject are embodied in the California Public Records Act (CPRA).[128] In passing the CPRA, the Legislature found that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[129] The law mandates disclosure of all public records,[130] except those "exempt from disclosure by express provisions of law."[131]

Thus, in applying the CPRA, the official must determine (a) whether the information is in a public record, as defined by the CPRA; (b) whether some doctrine preempts the CPRA and removes its public record status (for example, the right to privacy, see below); and (c) if it remains a public record, whether some statutory exemption in the CPRA removes it from the requirement of public disclosure.

Officials should note the consequences of applying the CPRA: If a record is covered and not exempt from disclosure, then obviously the question of whether the official may disclose the information is moot, because the official must disclose the information if asked to do so. If the record is ultimately determined not to be a public record under the CPRA,

---

[128] CAL. GOV'T CODE § 6250 et seq. (2009).

[129] *Id.*

[130] *See id.* § 6253(a)-(e) for guidelines on the process of accessing records, including time limits.

[131] *Id.* § 6253(b).

other rules may determine whether the official must or may disclose it. Officials should also note that the CPRA overlaps with the so-called "official information privilege," which is discussed in section A2 below. In many instances, if information is immune to disclosure under the CPRA it also falls within the scope of the official information privilege, and need not be disclosed.

1. What Constitutes a Public Record?

The CPRA defines a "public record" as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[132] A "writing" is:

> any handwriting, typewriting, printing, photostatting, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.[133]

Officials should note that this definition focuses not on information per se, but on a written *recording* of information. Therefore, officials should not think of the information in the abstract, and in seeking to comply with the CPRA, they should not consider whether the content of the record in question might be available from some other source outside the agency's purview. Even if the content is available in some alternative manner, the official's duty is to consider whether the documentation of the information within her agency's database constitutes a public record or not.

The meaning of "writing," therefore, becomes particularly important. Because the definition is both broad and vague, it is often a challenge to determine what constitutes a public record. Facing this challenge, courts must reconcile "two fundamental if somewhat competing societal concerns—prevention of secrecy in government and protection of individual privacy."[134] Generally, courts are more inclined to find that a contested document *is* a public record, presuming (subject to the

[132] *Id.* § 6252(e).
[133] *Id.* § 6252(g).
[134] Black Panther Party v. Kehoe, 42 Cal. App. 3d 645, 651 (Ct. App. 1974).

exemptions below) that disclosure is necessary.[135] This presumption is even stronger with regards to records in the criminal justice system. Thus, courts have required the disclosure of the identities of anyone with a criminal conviction working in a child day care facility, the names and employment information of peace officers, and the highway patrol's procedural regulations governing the investigation of citizen complaints.[136]

In cases where courts have held that the documents *are not* public records, there is generally a strong countervailing interest, such as the right to privacy. In *Oziel v. Superior Court*, 223 Cal. App. 3d 1284 (1990), the court held that a videotape of a warrant-based search of a psychotherapist's home and office was not a public record, primarily because disclosure violated the psychotherapist's right to privacy and right to be free of unreasonable searches and seizures under the Fourth Amendment. Technically speaking, these privacy rights are not "exemptions" under the CPRA itself. Rather, they have been construed as "superior" doctrines that preempt application of the CPRA, and its presumption for disclosure.[137]

The right to privacy, however, can be waived. In *Register Division of Freedom Newspapers, Inc. v. County of Orange*, 158 Cal. App. 3d 893 (1984), a court required disclosure of an inmate's medical records after the inmate reached a secret settlement in a lawsuit with the county. The court emphasized that by voluntarily submitting his medical records in order to reach a settlement, the inmate waived any expectation of privacy regarding those records.

Similarly, a strong "private function" may militate in favor of finding that the contested documents are not public records. A "private function" generally means that the documents do not relate to the "public's business," or are related to an activity that is "adversarial to and independent of the state."[138] In *Coronado Police Officers Association v.*

---

[135] *See* Vallejos v. California Highway Patrol, 89 Cal. App. 3d 781, 784 (Ct. App. 1979) ("[T]he general policy of the PRA favors disclosure").

[136] Comm'n on Peace Officer Standards and Training v. Superior Court, 42 Cal. 4th 278 (2007); CBS Broad., Inc. v. Superior Court, 91 Cal. App. 4th 892 (Ct. App. 2001); Cook v. Craig, 55 Cal. App. 3d 773 (Ct. App. 1976).

[137] Note that the application of the state right to privacy or the Fourth Amendment that removes the information from required CPRA disclosure does not necessarily indicate whether the official is forbidden from disseminating the information or if they will face liability for disclosure under state or federal law.

[138] Coronado Police Officers Ass'n v. Carroll, 106 Cal. App. 4th 1001, 1006, 1007 (Ct. App. 2003).

Carroll, 106 Cal. App. 4th 1001 (2003), the court held that a database compiled and maintained by the public defender's Office was not a public record because "its core function—the provision of adequate representation to indigent criminal defendants—was a private function rather than a public function."[139] The court likened the actions of the public defender's office to the traditional functions of private defense counsel.[140]

2. Examples of Public Records

California courts have held that the following documents *are* public records. As noted where relevant, these documents are not exempted by the CPRA—discussed in more detail below:

a. Convictions Relating to Childcare Work

The Department of Social Services (DSS) must disclose the identity of every individual who receives an exemption from a prior criminal conviction to work in a licensed child day care facility. DSS must also disclose the identity of each facility employing such individuals. The public has "an overwhelming interest" in making sure that DSS does not abuse its discretion in granting these exemptions.[141] In comparison to the public interest in disclosure, an individual's privacy interests are low, both because past convictions are a matter of public record, and because the individual invited public scrutiny when she applied for exemption. DSS disclosure, it should be noted, does not include a birth date or a physical description of the individual granted an exemption.[142]

b. Peace Officers' Names and Employment Information

The California Commission on Peace Officer Standards and Training must disclose the names and current employment information of all California peace officers. Such disclosure is permissible because the peace officers' names, employing agencies, and employment dates are not

---

[139] *Id.* at 1006 (Contrast this with the holding in *County of Santa Clara v. Superior Court*, 89 Cal. Rptr. 3d 374 (Ct. App. 2009), in which the county did not even contest whether a basemap it had compiled to provide extensive information about property parcels was a public record).

[140] *Coronado Police Officers Ass'n*, 106 Cal. App. 4th at 1008.

[141] *CBS Broad., Inc.*, 91 Cal. App. 4th at 906.

[142] *Id.* at 908. The court added that the $43,000 expense to the government involved in compiling such a list was not so great as to militate against disclosure. *Id.* at 909.

confidential under the umbrella of "peace officer personnel records," which are otherwise protected by statute. Peace officer "employment histories," moreover, are only protected with regard to previous employment, not current employment status.[143]

c. Highway Patrol Procedural Regulations Governing Citizen Complaints

The California Highway Patrol (CHP) is required to disclose its procedural regulations governing the investigation of citizen complaints against CHP personnel.[144]

d. Traffic Accident Reports

The California Highway Patrol is required to release written traffic accident reports prepared and retained by the agency.[145]

e. Records of Settlements of Tort Claims Brought by County Jail Inmates

Each county is required to release documents related to settlements of tort claims brought by county jail inmates. These documents include: (1) the inmate's medical records; (2) the sheriff's investigation report; (3) the minutes from the settlement committee meeting, including deliberation of the claim; (4) any rough undated notes made by risk management staff; and (5) any remaining settlement records.[146]

3. Examples of Non-Public Records

California courts have determined that the following documents *are not* public records:

a. Public Defender's Office Database

A county Public Defender office is not required to provide access to a database it compiles and maintains. The database is not a public record because "its core function—the provision of adequate representation to

---

[143] Comm'n on Peace Officer Standards and Training v. Superior Court, 42 Cal. 4th 278 (2007).

[144] Cook v. Craig, 55 Cal. App. 3d 773 (Ct. App. 1976).

[145] Vallejos v. California Highway Patrol, 89 Cal. App. 3d 781, 783 (Ct. App. 1979).

[146] Register Div. of Freedom Newspapers, Inc. v. County of Orange, 158 Cal. App. 3d 893 (Ct. App. 1984).

indigent criminal defendants—is a private function rather than a public function." Even if the database were a public record, it would be exempt from disclosure under the "catch-all" exemption of the CPRA (§ 6255), discussed in detail below. The public interest in nondisclosure, in fact, outweighs any public interest in disclosure: the information contained in such a database is necessary to the Public Defender's function as counsel to indigent criminal defendants.[147]

b. Videotapes of Warrant Searches

The videotape of a warrant-based search of a home and office is not a public record, and disclosure may violate the privacy rights of the subject of the search.[148]

4. Statutory Exemptions from CPRA Disclosure Requirements

There are two sections of the CPRA that allow government agencies to refuse to disclose certain public records: §§ 6254 and 6255. Section 6254 lists dozens of highly specific exemptions for items such as preliminary drafts or personnel files. (Agencies should consult the statute for additional exemptions not discussed in Subpart 1, below.) Section 6255 provides a "catch-all" exemption to disclosure when "the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record." The party opposing disclosure under the CPRA bears the burden of proving that an exemption applies.

Consequently, an agency can avoid disclosure by (1) arguing that a document is not a public record under the general definitions discussed above; (2) resisting disclosure by relying on a specific exemption found in § 6254; or (3) asserting that a document falls within the "catch-all" exemption provision of § 6255. Considerable overlap exists among these three grounds, and agencies often invoke more than one.

a. Specific Exemptions under CPRA Section 6254

Section 6254 includes a number of specially enumerated exemptions to disclosure obligations. Only those provisions relevant to criminal justice administration are addressed in this section. In some instances, section 6254 simply notes whole categories of information that are exempted from

[147] Coronado Police Officers Ass'n v. Carroll, 106 Cal. App. 4th 1001, 1006 (Ct. App. 2003).

[148] Oziel v. Superior Court, 223 Cal. App. 3d 1284 (Ct. App. 1990).

disclosure, even if that information otherwise meets the general definition of public records discussed above. In other instances, section 6254 recognizes that certain forms of information are public records, and presumptively must be disclosed, but will nevertheless exempt a subcategory of that information. Illustrative examples of the information affected by CPRA section 6254 includes the following:

- Agencies do *not* have to release the following: most preliminary drafts, notes, or memoranda;[149] records pertaining to pending litigation when the public agency is a party;[150] and personnel or medical files.[151]

- The Attorney General, the Department of Justice, any state or local police agency, and any other state or local agency acting for correctional or law enforcement purposes *do not* have to disclose records of complaints they have received or records of investigations they have conducted.

- Although agencies "shall disclose the names and addresses of persons involved in, or witnesses other than confidential informants to, the incident," as well as the statements of parties involved in the incident (except the statements of confidential informants), they do not have to disclose information that "would endanger the safety of a witness or other person involved in the investigation," or information that "would endanger the successful completion of the investigation or a related investigation." Agencies can also refuse to disclose any "portion of those investigative files that reflects the analysis or conclusions of the investigating officer."[152]

- There is a presumption that State and local law enforcement agencies must provide public access to information about individuals who are arrested. Law enforcement agencies, however, are exempt from such disclosure if it "would endanger the safety of a person involved in an investigation or would endanger the successful completion of the investigation or a related investigation." If this exception does not apply,

---

[149] CAL. GOV'T CODE § 6254(a) (2009) ("Preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the public agency in the ordinary course of business, if the public interest in withholding those records clearly outweighs the public interest in disclosure.").

[150] *Id.* § 6254(b) ("Records pertaining to pending litigation to which the public agency is a party . . . until the pending litigation or claim has been finally adjudicated or otherwise settled.").

[151] *Id.* § 6254(c) ("Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy.").

[152] *See id.* § 6254(f).

agencies should publicly disclose:

> The full name and occupation of every individual arrested by the agency, the individual's physical description including date of birth, color of eyes and hair, sex, height and weight, the time and date of arrest, the time and date of booking, the location of the arrest, the factual circumstances surrounding the arrest, the amount of bail set, the time and manner of release or the location where the individual is currently being held, and all charges the individual is being held upon, including any outstanding warrants from other jurisdictions and parole or probation holds.[153]

- Agencies are not required to release "criminal offender record information" (i.e., prior arrest records).[154]

- Criminal justice agencies must disclose the "time, substance, and location of all complaints or requests for assistance received by the agency" and "the time and nature of the response." Specifically, agencies must disclose "the time, date, and location of the occurrence, the time and date of the report, the name and age of the victim, the factual circumstances surrounding the crime or incident, and a general description of any injuries, property, or weapons involved."[155] As discussed above, the Victims' Bill of Rights (VBR) has superseded this provision and prohibits the disclosure of a victim's name and identifying information absent consent. (Note that courts have yet to interpret the VBR, so there is great uncertainty about the reach of its provisions. Until courts provide additional guidance about how to implement the VBR, agencies *should not release* victim information as discussed in Part IV.)

b. CPRA Section 6255: The "Catch-all" Balancing Test Exemption

Beyond the enumerated exemptions in Section 6254, the California Public Records Act provides a "catch-all" exemption for records meeting a general exemption standard—where "the public interest served by not disclosing the record clearly outweighs the public interest served by

---

[153] *Id.* § 6254(f)(1).

[154] Younger v. Berkeley City Council 45 Cal. App. 3d 825, 832 (Ct. App. 1975).

[155] CAL. GOV'T CODE § 6254(f)(2) (2009).

disclosure of the record."[156] The burden of proof falls on the government agency seeking to invoke this exemption and prevent disclosure.[157] Disclosure is strongly favored, and the agency must "demonstrate a clear overbalance on the side of confidentiality."[158] The inquiry is heavily case- and fact-specific.

A 2009 California appellate decision ordering Santa Clara County to fulfill a CPRA request for geographic information system (GIS) mapping data sheds some light on the balancing test courts use when assessing the "catch-all" exemption.[159] The county argued that public finances (the mapping data was valuable) and security concerns weighed against disclosure. The court disagreed, finding that the public interest in disclosure was "neither hypothetical nor minimal,"[160] as measured by "whether disclosure would contribute significantly to public understanding of government activities."[161] The court, moreover, thought the case could be differentiated from situations involving individual privacy concerns, as well as situations where "less intrusive means to obtain the information" existed.[162]

In assessing the public interest against disclosure, the court found little evidence that the government's financial concerns were legitimate, and noted that the CPRA did not "suggest that a records request must impose no burden on the government agency."[163] Addressing the security concerns, the court noted that the county had sold the data to other entities, and found that the GIS did not primarily contain information with national-security

---

[156] CAL. GOV'T CODE §6255(a) (2009).

[157] New York Times Co. v. Superior Court, 218 Cal. App. 3d 1579, 1584 (Ct. App. 1990).

[158] Michaelis, Montinari & Johnson v. Superior Court, 136 P.3d 194, 197 (Cal. 2006).

[159] County of Santa Clara v. Superior Court, 170 Cal. App. 4th 1301 (Ct. App. 2009). The court also denied the county's claim that the request was blocked not just by the CPRA catch-all exemption, but also under the federal Critical *Infra*structure Information (CII) Act.

[160] *Id.* at 1325.

[161] *Id.* at 1324 (quoting City of San Jose v. Superior Court, 74 Cal. App. 4th 1008, 1018 (1999)).

[162] *Id.* at 1325.

[163] *Id.* at 1327 (citing CBS Broad., Inc. v. Superior Court, 91 Cal. App. 4th 892, 909 (Ct. App. 2001), a case that held that the $43,000 cost of compiling the data was not "a valid reason to proscribe disclosure").

implications.[164] The CPRA's exemptions, the court held, cannot be applied to classify information that would otherwise be public.[165] Although security concerns could weigh heavily against disclosure, the "mere assertion of possible endangerment does not 'clearly outweigh' the public interest in access to these public records."[166]

The "catch-all" exemption, nevertheless, has been used to prevent disclosure of records in cases where an individual's right to privacy is at issue. For instance, a prisoner's records, sought by the media, are not considered public records subject to disclosure. In reaching this decision, a California court cited the prisoner's right to a trial free of unfair prejudice.[167]

5. Legal Remedies for Invalid *Non*-Disclosure under the CPRA

Because the purpose of the CPRA is to ensure access to non-exempt public records, the statute's remedies are intended to confront wrongful *nondisclosure*. These remedies are limited to injunctions or declarative relief,[168] and the award of attorney's fees in litigation if the plaintiff prevails.[169] Individual public officials, consequently, should not fear that they will be personally liable for damages if they erroneously refuse to disclose information that is ultimately determined to be a non-exempt public record.

Agencies, however, do have an affirmative burden to assist records requesters: they must "assist the member of the public to identify records and information that are responsive to the request or to the purpose of the request" and "provide suggestions for overcoming any practical basis for denying access to the records or information sought."[170] The provision sets forth a "reasonable effort" standard and does not apply if the public agency denies the request under one of the specific exemptions of CPRA § 6254 or if the agency makes available an index of its records.[171]

---

[164] *Id.* at 1329.
[165] *Id.* at 1321.
[166] *Id.* at 1329 (quoting CBS, Inc. v. Block, 42 Cal. 3d 646 (1986)).
[167] Yarish v. Nelson, 27 Cal. App. 3d 893 (Ct. App. 1972).
[168] CAL. GOV'T CODE § 6258 (2009).
[169] *Id.* § 6259(d).
[170] *Id.* § 6253.1(a).
[171] *Id.* § 6253.1(d).

Agencies should carefully consider what portions of their records are likely to be exempted under § 6254's specific provisions before relying on the "catch-all" exemption to protect data. Because a heavy burden falls on the government in "catch-all"-exemption litigation, such cases may be time-consuming, costly, and difficult to win. Moreover, because cost is not a justification for withholding data under the CPRA, and because the CPRA places affirmative obligations on agencies to assist record-seekers in their searches, agencies designing databases should consider technologies that will reduce the burden on employees in dealing with public-records requests.

B. Federal Statutes: FOIA, the Privacy Act, and the Information Practices Act

This section describes federal statutes that govern when information must be released (and by whom). FOIA and the Privacy Act apply to records held by the federal government—but it is included in this Primer because federal agencies often exchange information with local agencies. The Information Practices Act imposes limitations on exposing nonpublic information to the public, but the relief is primarily injunctive. Each shall be discussed in turn.

1. FOIA and the Privacy Act

The Freedom of Information Act ("FOIA")[172] and the Privacy Act[173] allow public access to records *held by the federal government*. The statutes are worth noting in this Primer because federal officials, whether or not they are located in California, may interact with state officials on some criminal justice matters. Nevertheless, these federal statutes have no direct application to state officials.

Like the CPRA, the FOIA provides an exemption for "records or information compiled for law enforcement purposes."[174] However, FOIA's exemption for investigatory data is much harder to claim: FOIA requires proof that investigatory information "would interfere with enforcement, threaten a fair trial, invade a person's privacy, disclose confidential information or sources, disclose investigative techniques, or endanger the

[172] 5 U.S.C. § 552 (2008).
[173] *Id.* § 552(a).
[174] *Id.* § 552(b)(7).

life of law enforcement personnel."[175] California state officials, consequently, have more discretion to avoid disclosure under the state law than federal officials do under the federal law.

Distinct from FOIA, the federal Privacy Act allows individuals to access their own federal records and to request that the record be changed if inaccurate.[176] It also places affirmative requirements on federal databases to contain accurate and timely information.[177] (These requirements do not apply to non-federal actors, unless the inability to petition for changes to inaccurate data rises to the level of a constitutional-rights violation.) The head of a federal agency may exempt that agency from many Privacy Act requirements, including those pertaining to accuracy, if the agency's database "performs as its principal function any activity pertaining to the enforcement of criminal laws."[178] The U.S. Department of Justice, for instance, chose in 2003 to exempt certain databases from accuracy requirements, including the National Crime Information Center.[179] In exempting the databases, the federal DOJ said that the "exemption is necessary to avoid interference with law enforcement functions and responsibilities of the FBI . . . because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete."[180]

Remedies under the Privacy Act, in cases where records have not been exempted, include injunctions or orders to amend the record and awards of attorney fees and costs if the plaintiff "substantially" prevails; if the agency acted intentionally or willfully, actual damages will also be awarded.[181] Damages are often limited, however, because of the requirement that they be actual, provable damages. For instance, the Supreme Court overturned an award for disclosure of a plaintiff's social security number because the plaintiff could not prove the disclosure resulted in actual damages.[182] Criminal penalties are also available against federal agency employees who

---

[175] Williams v. Superior Court, 5 Cal. 4th 337, 349 (1993).

[176] 5 U.S.C. § 552a(d)(1)-(2).

[177] *Id.* § 552a(e)(5).

[178] *Id.* § 552a(j)(2).

[179] Exemption of Federal Bureau of Investigation Systems, 16 C.F.R. § 16.96 (2003).

[180] 68 Fed. Reg. 14140 (Mar. 24, 2003) (to be codified at 28 C.F.R. pt. 16).

[181] 5 U.S.C. § 552a(g).

[182] Doe v. Chao, 540 U.S. 614 (2004).

willfully and wrongfully disclose data.[183]

2. The Information Practices Act

The Information Practices Act (IPA) "generally imposes limitations on the right of governmental agencies to disclose personal information about an individual."[184] Except for specifically enumerated exceptions, "[n]o agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains."[185] The IPA, therefore, operates as a specific statutory version of the right to privacy. Violations may result in an injunction;[186] damages are only applicable when someone "other than an employee of the state or of a local government agency acting solely in his or her official capacity" discloses nonpublic information knowing it was maintained by a government agency.[187]

The IPA is unlikely to create many difficulties for information-sharing efforts. First, the IPA permits disclosure for a legitimate purpose and balances "the intrusion [on privacy] against the public interests to be served."[188] The handful of cases brought under the IPA concern agencies or individuals who disclosed information for no legitimate agency purpose.[189]

Second, and most important, the IPA specifically permits intra- and inter-agency disclosure. The IPA permits *intra-agency* disclosure "[t]o those officers, employees, attorneys, agents, or volunteers of the agency that has custody of the information," insofar as the disclosure is relevant and necessary for official duties and is related to the purpose for which it was acquired.[190] It also permits *inter-agency* disclosure to a person or other agency when it is needed for the transferee to "perform its constitutional or statutory duties" and the use is compatible with the purpose for which it was collected. The statute simply requires that the transferring agency maintain

---

[183] 5 U.S.C. § 552a(i).

[184] Bates v. Franchise Tax Bd., 21 Cal. Rptr. 3d 285, 287 (Ct. App. 2004).

[185] *Id.* § 1798.24.

[186] CAL. CIV. CODE § 1798.47 (2009).

[187] *Id.* § 1798.53.

[188] People v. McCray, 50 Cal. Rptr. 3d 343 (Ct. App. 2006) (internal citation omitted).

[189] *See, e.g.*, Anti-Defamation League of B'nai B'rith v. Superior Court, 79 Cal. Rptr. 2d 597 (Ct. App. 1998) (allowing discovery in suit against defendant journalist who solicited and received nonpublic information from the police).

[190] CAL. CIV. CODE § 1798.24(c) (2009).

a record of disclosure that includes the date, nature of the disclosed information, and purpose of the disclosure, as well as the name, title, and business address of the person or agency to which the disclosure was made.[191]

These permitted disclosures are exceptionally broad. They apply where receipt of the information is relevant to the agency or sub-agency's function and therefore would clearly apply whenever a criminal justice agency wishes to share information with another governmental agency for purposes relevant to criminal justice.

VI. LITIGATION ISSUES IN PROSECUTION

This Part deals with issues that might come up during the prosecution of defendants in criminal cases. There are three examples that are considered, in sections A, B, and C respectively. The first concerns whether reliance on inaccurate data in the issuance or execution of search warrants might result in suppression of evidence. The second, in section B, concerns the prosecution's obligation under *Brady* to turn over exculpatory evidence. Information sharing widens the pool of information which might potentially exculpate defendants, and thus creates challenges for *Brady* compliance. The third, in section C, concerns evidentiary privilege rules—the complex rules concerning when an individual (or an entity) may not disclose private information. Each will be discussed in turn.

A. Reliance on Inaccurate Data and Evidentiary Exclusion

The subject of searches and seizures under the Fourth Amendment, and the requirement of probable cause for arrest, comprises a vast body of legal doctrine—far beyond the scope of this Primer. Nevertheless, one issue related to searches and seizures is a very salient one for agency officials and employees--most obviously those in law enforcement and the judiciary--dealing with individualized data. This is the issue of the consequences of officials' reliance on inaccurate data when executing an arrest or a carrying out a search. The issue arises especially when police act under the authority of a warrant. A warrant is actually not required for the majority of arrests and for some cases of searches, but warrants play an important role in cases of "teamwork," where some officials do not possess the original source of information, but instead are "downstream" receivers of information ultimately certified in a warrant.

---

[191] *Id.* § 1798.25.

The bottom line is clear: police, prosecutors, and judicial officials probably need not even fear loss of admissible evidence when their actions rest on inaccurate data. They must, however, have a good faith, "objectively reasonable basis" for their belief in the accuracy of that data.

Reliance on inaccurate data can threaten the legality of police conduct under the Fourth Amendment. Arrests and searches normally must be based on an inference from available facts that there is probable cause to believe the person has committed a crime, or, in the case of a search, that evidence of the crime is present in the place to be searched. Therefore, if the police have drawn the inference of probable cause from false data, probable cause may not exist.

Most of the Supreme Court's Fourth Amendment case law bears on one major consequence of a violation of Fourth Amendment rights—suppression of evidence in a criminal proceeding, under the exclusionary rule.

But the retrospective determination that the inference of probable cause rested on mistaken information will not necessarily render the evidence subject to the exclusionary rule. The Supreme Court confirmed the "good faith exception" to the exclusionary rule in *United States v. Leon*.[192] There, a magistrate negligently issued a warrant on the basis of an affidavit that, in retrospect, was deemed insufficient to support probable cause. The Court held that the evidence seized under the warrant need not be suppressed because the police reasonably relied on the magistrate's judgment.[193] In 1995, the Court extended this doctrine in *Arizona v. Evans*, to a case where the error was not the probable cause for the warrant but the very existence of a warrant: the police had relied on a judicial database that had failed to record the expiration of an old warrant.[194]

But the application of this doctrine to errors by law enforcement itself was just recently resolved by the Supreme Court in *Herring v. United States*.[195] *Herring* involved an erroneous record of an expired warrant, but the error was by the police agency itself. The Court held that if an officer *reasonably believes* there is an outstanding arrest warrant on an individual, but that belief turns out to be wrong because of a negligent bookkeeping

[192] 468 U.S. 897 (1984).
[193] *Id.* at 913.
[194] Arizona v. Evans, 514 U.S. 1, 14-15 (1995).
[195] 129 S. Ct. 695 (2009).

error by another police employee, evidence found during the subsequent search-incident-to-arrest need not be suppressed.[196] As the Court noted, the rationale underlying the exclusionary rule is that exclusion rule is a prophylactic remedy intended to deter misconduct. The exclusionary rule is not an individual right: It applies only where the "benefits of deterrence . . . outweigh the costs."[197] The Court determined in *Herring* that the costs of applying the exclusionary rule to negligent errors outweigh the benefits, since the negligent conduct is not "sufficiently deliberate that exclusion can meaningfully deter it."[198]

If, however, police mistakes are the result of "systemic error or reckless disregard of constitutional requirements," resulting evidence may, in fact, be excluded.[199] Thus, to avoid suppression of evidence, police departments should establish reliable databases and consistent recordkeeping methods to avoid a finding of systemic error or recklessness in maintaining a warrant system. Moreover, if any employee of the police department "knowingly [makes] false entries to lay the groundwork for future false arrests," a court would surely exclude the evidence.[200]

Evidence gained in reliance on inaccurate information from *judicial* employees is even less likely to be excluded. First, when police rely on mistaken information in a court's database that an arrest warrant is outstanding, evidence resulting from the subsequent search-incident-to-arrest is not subject to exclusion.[201] Thus, the exclusionary rule does not apply when a judicial employee makes a negligent error. In *Arizona v. Evans*, the Court reasoned that (1) the exclusionary rule was historically designed to deter police misconduct, not errors by clerks, judges or magistrates; (2) there was no evidence that judicial employees were inclined to subvert the Fourth Amendment; and (3) there was no basis for believing that suppressing the evidence would have a significant deterrent effect on judicial employees.[202]

B. The Prosecutor's Duty to Disclose Under Brady

Every lawyer should know the constitutional rule established in

---

[196] *Id.* at 698.
[197] *Id.* at 700.
[198] *Id.* at 702.
[199] *Id.* at 704.
[200] *Id.* at 703.
[201] Arizona v. Evans, 514 U.S. 1, 14-15 (1995).
[202] *See id.*

Brady v. Maryland, requiring prosecutors to turn over relevant "exculpatory" information to a defendant. Exculpatory information weighs in favor of the defendant's innocence.[203] Every California prosecutor, similarly, should know she is subject to additional state rules and policies governing discovery in criminal litigation. In effect, these discovery laws constitute a special subcategory of "information sharing" rules, and they merit discussion in this Primer.

New developments in electronic databases and information-sharing in and among public agencies have complicated criminal discovery rules. The developments also require prosecutors to consider the *Brady* doctrine in coordination with the other rules governing criminal justice data sharing discussed in this Primer. Prosecutors who are mindful of their obligations to disclose exculpatory information to defendants may have augmented responsibilities if they partake in an integrated criminal justice information system. Put differently, *Brady*-type rules must be placed in a holistic picture of the criminal justice system.

1. The Duty to Disclose

The prosecutor's core responsibilities do not change in an electronic data-sharing environment. Whenever criminal justice agencies enter into data-sharing agreements that include prosecutors—and thereby integrate themselves into what courts have termed the "prosecution team" (agencies that aid the prosecutor in performing a prosecutorial function)—the participating prosecutors are responsible for disclosing any material exculpatory information to the defendant that the integrated agencies possess, even if these agencies do not call the exculpatory information to the prosecutor's attention. Consequently, a prosecutor that is concerned with minimizing his or her liability for not disclosing exculpatory information will be reluctant to participate in an integrated criminal justice information system.

At least three layers of rules mandate the prosecutor's duty to disclose:

a. Federal Due Process Requirements

[203] 373 U.S. 83 (1963) ("[T]he suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or punishment, irrespective of the good faith or bad faith of the prosecutor.").

In general, defendants do not have a constitutional right to discovery in criminal proceedings.[204] In *Brady v. Maryland*, the United States Supreme Court recognized that defendants have a due process right to discover "exculpatory evidence" in a criminal case.[205] It is a violation of a defendant's due process rights for a prosecutor to suppress exculpatory evidence, regardless of whether the suppression is intentional or inadvertent. In post-*Brady* cases, the Court has construed the term "exculpatory" to cover a wide variety of information, including all information that has a minimally plausible potential to aid the defense in creating reasonable doubt of guilt.[206] Even evidence that *favors the prosecutor* may be "exculpatory" if timely awareness of it would help the defense prepare to rebut it or to impeach the state's witnesses.[207] Although the *Brady* doctrine does not set down strict timing rules, prosecutors must provide exculpatory evidence in time to give the accused a reasonable opportunity to benefit from it at trial, and prosecutors are well-advised to continue to disclose any such exculpatory evidence even during plea bargain negotiations and after trial, pending appeal.[208]

---

[204] Weatherford v. Bursey, 429 U.S. 545, 559 (1977).

[205] *Brady*, 373 U.S. at 87 ("[T]he suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or punishment, irrespective of the good faith or bad faith of the prosecutor.").

[206] United States v. Bagley, 473 U.S. 667, 682 (1985) (evidence is considered material if "there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different.").

Criminal cases are invariably complicated and what constitutes material exculpatory evidence in a specific case is based on the specific facts of the case. But common types of material exculpatory evidence include: (1) promises of immunity or other favorable treatment to government witnesses; (2) prior criminal records of government witnesses; (3) prior inconsistent statements of government witnesses regarding the defendant's alleged criminal conduct; (4) prior perjury or false testimony of government witnesses; (5) monetary rewards or inducements to government witnesses; (6) confessions to the crime in question by others; (7) information reflecting bias or prejudice by government witnesses against the defendant; (8) witness statements that others committed the crime in question; (9) information about mental or physical impairments of government witnesses; (10) inconsistent or contradictory examinations or scientific tests; and (11) the failure of any percipient witnesses to make a positive identification of the defendant. *See, e.g.*, American College of Trial Lawyers, *Proposed Codification of Disclosure of Favorable Information Under Federal Rules of Criminal Procedure 11 and 16*, 41 AM. CRIM. L. REV. 93, 102-03 (2004).

[207] Giglio v. United States, 405 U.S. 150, 153-54 (1972) (favorable evidence to the defendant includes impeachment evidence).

[208] In any event, California prosecutors are under more specific timing

The Court has also held that the prosecutor has an affirmative duty to look for exculpatory evidence held by various partner law enforcement agencies, including the police.[209] The prosecutor must disclose the exculpatory evidence to the defendant regardless of whether the defendant made a specific discovery request for exculpatory material evidence.[210] Finally, and most importantly for integrated criminal justice information systems, the Supreme Court has held that "the individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police."[211]

The *Brady* doctrine does not by itself impose any personal liability on government officials for failing to comply with their discovery duties. The constitutionally prescribed remedy, however indirect, is still powerful. If, on appeal after conviction, the defendant can establish a failure to turn over material exculpatory evidence, the appellate court must reverse the conviction if there is any reasonable probability that the withheld information would have affected the verdict—i.e., if there is any reasonable probability that the jury (or judge, in a bench trial), informed by the evidence in question, would have acquitted on any count of conviction. This retrospective conception of the *Brady* rule might, in marginal cases, make it hard for prosecutors to comply. In effect, the very definition of what makes evidence material and exculpatory depends on this retrospective view, yet as the state's case evolves during trial itself, it may be difficult to predict whether evidence would affect the ultimate verdict. Nevertheless, the professional ethics codes and California state laws counsel that prosecutors err well on the side of timely disclosure before or during trial to avoid sanctions and possible reversal.

b. American Bar Association and California Model Rules of Professional Conduct

Under the American Bar Association and California Model Rules of Professional Conduct, a prosecutor must provide the defense with exculpatory evidence during trial and mitigating evidence during sentencing.[212] A prosecutor is prohibited from suppressing any evidence

---

obligations under state law; *see* Subparts 1 and 3 of this Part.

[209] Kyles v. Whitely, 514 U.S. 419, 437 (1995).

[210] United States v. Agurs, 427 U.S. 97, 107 (1976).

[211] *Kyles*, 514 U.S. at 437.

[212] MODEL RULES OF PROF'L CONDUCT, R. 3.8(d) (2002).

that he or she is legally obligated to disclose to the defense.[213] A failure to disclose exculpatory information may constitute a violation of the California Rules of Professional Conduct[214] and other ethical standards,[215] and therefore lead to professional disciplinary sanctions.

c. California Statutory Requirements

In California, the prosecutor's duty to disclose exculpatory evidence mirrors the prosecutor's obligations under *Brady*.[216] Similar to *Brady*, Penal Code Section 1054.1(e) acts as a foundation that establishes the prosecutor's basic discovery obligations. Various California courts have issued opinions to demarcate a prosecutor's disclosure obligations under Penal Code Sections 1054 et seq. In general, the statutory requirements do not impose a greater duty on the prosecutor to disclose favorable evidence to the defense.[217] *In re Littlefield*, for example, holds that the prosecution must disclose exculpatory information when it is reasonably accessible to the prosecution and not accessible to the defense.[218] In addition, *Izazaga v. Superior Court*, reaffirming the holding in *United States v. Agurs*, explained that a prosecutor has a duty to disclose exculpatory evidence regardless of whether a discovery request is made by the defendant.[219]

California courts have also noted that "the duty of the prosecuting

---

[213] CALIFORNIA RULES OF PROF'L CONDUCT, R. 5-220 (1992).

[214] *See id*. (Rule 5-220 Suppression of Evidence describes that **"**[a] member shall not suppress any evidence that the member or the member's client has a legal obligation to reveal or to produce").

[215] MODEL RULES OF PROF'L CONDUCT, PREAMBLE AND SCOPE: A LAWYER'S RESPONSIBILITIES (2002); *see also* ABA CRIMINAL JUSTICE SECTION STANDARDS, PROSECUTORIAL FUNCTION, STANDARD 3-3.1 (1992); MODEL RULES OF PROF'L CONDUCT, R. 8.4(A) (2002).

[216] 5 WITKIN CAL. CRIM. LAW CRIM TRIAL § 41 (2008); *see also id.* § 550; CAL. PENAL CODE § 1054.1(E) (2008); 3-70 CALIFORNIA CRIMINAL DEFENSE PRACTICE § 70.03 (2008) ("Penal Code Section 1054.1(e) requires the prosecution to disclose to the defense 'any exculpatory evidence.' This requirement does not supersede or limit the prosecution's duty under the Federal Constitution to disclose all substantial material evidence favorable to the accused.").

[217] *See, e.g.*, People v. Zambrano, 41 Cal. 4th 1082, 1133-1134 (2007), *overruled, in part, by* People v. Doolin, 45 Cal. 4th 390, 421 (2009).

[218] *See, e.g.*, In re Littlefield, 5 Cal. 4th 122 (1993); People v. Coyer, 142 Cal. App. 3d 839, 843 (Ct. App. 1983). *See generally* 5 WITKIN CAL. CRIM. LAW CRIM TRIAL § 70 (2008).

[219] Izazaga v. Superior Court, 54 Cal. 3d 356 (1991).

attorney to disclose exculpatory evidence does not end when the trial is over."[220] A prosecutor's obligations to disclose material exculpatory information spans the entire life of a criminal case. Finally, state courts have clarified that a prosecutor is deemed to possess exculpatory evidence if the information is actually held by an agency that has assisted the criminal prosecution or investigation. The major consideration in this regard is whether the agency has been "acting on the government's behalf."[221]

2. The Prosecutor's Duty to Disclose Exculpatory Information When She Has Access to Integrated Criminal Justice Information Systems

Wider access to criminal justice information can change the scope of the prosecutor's duty to disclose exculpatory information. It can do so by increasing the amount of information to be reviewed, leading to concerns over how prosecutors are to be guided in what to disclose and how and when to disclose it. Second, a tightly-integrated criminal justice information system might expand the definition of the prosecution team itself to include law enforcement. This might mean that, say, a local police department might be unaware it has *Brady* obligations and fail to turn over evidence. After discussing these two concerns, this section goes on to consider possible responses to them and to discuss how information exchange might make *Brady* compliance more efficient.

---

[220] *See* CALIFORNIA CRIMINAL LAW PROCEDURE AND PRACTICE § 11.31 (Cal CEB 2008); 5 WITKIN CAL. CRIM. LAW CRIM TRIAL § 34 (2008) (discussing proceedings covered under the provisions of Penal Code 1054 et seq.); 5 WITKIN CAL. CRIM. LAW CRIM TRIAL § 78 (2008) (citing People v. Garcia, 17 Cal. 4th 1169, 1179 (1993)).

[221] People v. Superior Court (Barrett), 80 Cal. App. 4th 1305, 1315 (Ct. App. 2000) ("The scope of the prosecutorial duty to disclose encompasses exculpatory evidence possessed by investigative agencies to which the prosecutor has reasonable access. A prosecutor has a duty to search for and disclose exculpatory evidence if the evidence is possessed by a person or agency that has been used by the prosecutor or investigating agency to assist the prosecution or the investigation agency in its work. The important determination is whether the person or agency has been 'acting on the government's behalf.' Conversely, a prosecutor does not have a duty to disclose exculpatory evidence or information to a defendant unless the prosecution team actually or constructively possesses the evidence or information. Thus, information possessed by an agency that has no connection to the investigation or prosecution of the criminal charge against the defendant is not possessed by the prosecution team, and the prosecutor does not have the duty to search for or to disclose such material.").

a. The scope of "exculpatory" or "material" information

In the absence of a prosecutor's willful decision to suppress obvious, readily accessible exculpatory information, most *Brady* material is neither easily identifiable nor readily attainable. Even where electronic data-sharing makes information more accessible, the exculpatory content of that information remains difficult to discern. In many cases, office guidelines instruct federal and state prosecutors how to handle the discovery of *Brady* material, but are not standardized or sufficiently instructive.[222] As a result, individual prosecutors wield substantial discretion in determining how to manage their discovery obligations under *Brady* and Penal Code Section 1054.1(e). A prosecutor can withhold evidence if the prosecutor believes that there is a reasonable probability that the information will not affect the jury verdict, and this requirement does not change simply because the formatting of information is electronic.

This "gamesmanship" problem is most evident in the scenario where the defense does not make a specific discovery request for exculpatory material. In these situations the prosecutor is given no outside structure through which to determine what information would likely assist the defense in building an effective defense. The prosecutor is not required to give the defense everything the defense could conceivably wish to receive,[223] but she may be forced to make difficult judgment calls as to whether evidence is helpful or material. Courts encourage prosecutors to disclose information that may be exculpatory—and, in fact, a prosecutor is free to share any non-privileged information—but not all prosecutors will want to unnecessarily buttress a defense case with information that is ultimately just "helpful" to the defense.

---

[222] *See, e.g.*, CALIFORNIA COMMISSION ON THE FAIR ADMINISTRATION OF JUSTICE, BRADY LAW AND POLICY: VENTURA COUNTY (July 6, 2007), *available at* http://www.ccfaj.org/documents/reports/prosecutorial/expert/Ventura%20Brady%20outline.pdf (last visited Mar. 20, 2009); CALIFORNIA COMMISSION ON THE FAIR ADMINISTRATION OF JUSTICE, OFFICIAL REPORT AND RECOMMENDATIONS ON PROSECUTORIAL DUTY TO DISCLOSE EXCULPATORY EVIDENCE, *available at* http://www.ccfaj.org/documents/reports/prosecutorial/official/OFFICIAL%20REPORT%20ON%20BRADY%20COMPLIANCE.pdf (last visited Mar. 20, 2009).

[223] *In re* Littlefield, 5 Cal. 4th 122, 135 (1993) ("[T]he prosecution has no *general duty* to seek out, obtain, and disclose all evidence that might be beneficial to the defense."). *See also In re* Imbler, 60 Cal. 2d 554, 569 (1963) ("Although representatives of the state may not suppress substantial material evidence, they are under no duty to report *sua sponte* to the defendant all that they learn about the case and about their witnesses.").

The good faith attempt to identify and disclose reasonably accessible exculpatory material to the accused—but not to share helpful material—may be viewed by others as a deliberate attempt to circumvent the requirements of *Brady* and its progeny. What further complicates this problem is that it is hard for a prosecutor to identify favorable information at the outset of a trial when he or she has no idea how the issues will actually play out at trial. As is often the case with alleged *Brady* violations, evidence that a prosecutor categorizes as non-discoverable before the trial may prove to be material evidence at later stages in the case.

In many instances, consequently, the prosecutor may simply guess wrong whether evidence is material, while in other instances the prosecutor might arguably be guilty of hedging against certain information getting uncovered. Amidst these dilemmas, robust information sharing platforms are likely to increase the frequency with which a prosecutor is forced to make materiality determinations, as the universe of potentially exculpatory information will certainly expand.

b. Expanding the "Prosecution Team" and the Prosecutor's Responsibilities

In addition to the identification issue, a separate dilemma for prosecutors arises in an electronic data-sharing environment when more parties are grouped as members of the prosecution team.[224] Not only is the universe of information likely to be characterized as reasonably accessible, but the agencies possessing the information may also be characterized as engaging in a prosecutorial function. Namely, a prosecutor that has systematic and formal data sharing access to information compiled by local criminal justice agencies is arguably incorporating those agencies into the prosecution team, even if they are not instrumental to a prosecutorial or investigative function. (Under *Brady*, information possessed by an agency that has no connection to the investigation or prosecution, and is not part of an information-sharing agreement, is not possessed by the prosecution team, and, thus, the prosecutor does not have a duty to search for or to disclose such material.)

In this regard, a prosecutor's participation in a comprehensive

[224] Members of the prosecution team include any federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. Kyles v. Whitley, 514 U.S. 419, 437 (1995).

information sharing system may unwittingly expand the prosecutor's obligations to account for the information of other agencies now incorporated into the prosecution team.[225] While the prosecutor's disclosure obligations do not change in a formalized data-sharing environment, the universe of readily accessible information for which the prosecutor is liable is expanded.[226] As a practical matter, the prosecutor faces an increased risk of overlooking relevant information and exhibiting negligence if she does not micromanage the other agencies. In all likelihood, though, a prosecutor will demonstrate competence in seeking out exculpatory information that is maintained in an integrated information database.

c. An Open File Policy as a Remedy for Gamesmanship?

Prosecutors are not required to adopt an open file policy,[227] but prosecutors may increasingly elect to use an open file discovery policy in the context of electronic data-sharing. The gamesmanship problem remains a concern when a prosecutor adopts an open file policy because the open file policy may be employed as a tool to subvert the prosecutor's duty to disclose *Brady* material.[228] While an open file policy, in some sense, may enhance the perception of compliance, the underlying concern is that a prosecutor is still able to withhold information that is presented in an open file.[229]

As a practical matter, an open file policy is most useful when the information in the file is accurate and complete. Therefore, a prosecutor who makes no effort to supplement the information in the file or to ensure that the open file is actually representative of the information that they can access will distort the discovery process and violate a defendant's due

---

[225] The prosecution's obligations will remain the same with respect to entities that are traditionally considered part of the prosecution team even if the latter entities do not partake in the information sharing network.

[226] *See, e.g.*, People v. Johnson, 142 Cal. App. 4th 776 (Ct. App. 2006) (police reports concerning impeachment evidence not in an electronic database, Criminal Justice Information System, that defense counsel had access to and prosecutor did not provide defense with missing police reports in violation of *Brady*).

[227] *Kyles*, 514 U.S. at 437 ("We have never held that the Constitution demands an open file policy.").

[228] *See, e.g.*, People v. Zambrano, 41 Cal. 4th 1082, 1134 (2007) *overruled, in part, by* People v. Doolin, 45 Cal. 4th 390, 421 (2009).

[229] *See, e.g.*, Banks v. Dretke, 540 U.S. 668 (2004).

process rights.[230] The prosecutor would not satisfy his *Brady* discovery obligations by simply relying on a participating agency to update a shared database; the responsibility to disclose is uniquely the prosecutor's obligation.[231] For instance, information that is in the process of being uploaded into a database is still subject to the *Brady* rules.[232]

As a result, an open file policy does not necessarily obviate a prosecutor's duty to disclose exculpatory materials not contained in the open file; but an open file policy can effectively lessen the suspicion that a prosecutor is withholding information. Perceptions of compliance aside, if a prosecutor is responsible for disclosing exculpatory information held by integrated agencies, it may be most practical for the prosecutor to provide the defendant with access to the entire file. Some commentators express concern that an open file policy may be used as a tactic to overwhelm the defense with information.[233] In the context of an electronic database, however, it may be quite easy for a defense counsel to key word search through the electronic file. In this sense, an integrated database of information may facilitate the discovery of *Brady* material.

---

[230] This problem is compounded by the fact that a defendant is unlikely to know whether a file is complete and may actually gain a false confidence from having access to the prosecutor's open file regarding how to proceed at trial. In effect, the defendant is in the same position as when the prosecutor informs the defense that there is no exculpatory evidence. The defense has no real way to measure how forthright the prosecutor is in representing compliance with the discovery rules. Moreover, as the Supreme Court noted in *Bagley*, this type of misrepresentation can cause detrimental reliance on the part of the defense, e.g., "the defense might abandon lines of independent investigation, defenses, or trial strategies that it otherwise would have pursued." United States v. Bagley, 473 U.S. 667, 682 (1985).

[231] *See e.g.*, *In re* Brown, 17 Cal. 4th 873 (1998) ("[T]he Supreme Court has unambiguously assigned the duty to disclose solely and exclusively to the prosecution; those assisting the government's case are no more than agents. By necessary implication, the duty is nondelegable at least to the extent the prosecution remains responsible for any lapse in compliance. Since the prosecution must bear the consequences of its own failure to disclose, a fortiori, it must be charged with any negligence on the part of other agencies acting on its behalf.").

[232] *Id*. at 881 ("The principles *Brady* and its progeny embody are not abstractions or matters of technical compliance. The sole purpose is to ensure that the defendant has all available exculpatory evidence to mount a defense. To that end, a document sent but not received is as useless as a document not sent at all.").

[233]Bennett L. Gershman, *Litigating Brady v. Maryland: Games Prosecutors Play*, 57 CASE W. RES. L. REV. 531 (2007).

Given the likelihood that criminal justice agency files are not always in synch with a prosecutor's file (for instance, due to delays in uploading information), an open file policy in an integrated information database may provide a defendant with wholly accurate and reliable information at one point but incomplete and misrepresentative information at another. A defense attorney will likely be aware of this pitfall, as discussed earlier, but it is not the defense attorney's responsibility to micromanage a prosecutor's discovery obligations.

d. Improved Efficiency and Quality of Information

Although an integrated information system may make some of the gamesmanship problems more pronounced, an integrated information system could also enable the prosecutor to more efficiently meet his or her *Brady* disclosure requirements.[234] Assuming a prosecutor seeks a fair adjudicative process and demonstrates a willingness to act in good faith, an electronic data-sharing environment can facilitate prompt compliance with *Brady* and comparable discovery rules. The vast amount of information that a prosecutor is obligated to sift through would become more easily navigable if aligned criminal justice agencies (i.e., agencies that would normally be considered part of the prosecution team) participate in integrated criminal justice information sharing systems.

The effectiveness of discovery rules established by *Brady* and under Penal Code Sections 1054 et seq. ultimately depends on the individual attitudes and posture of a prosecutor. It may seem counterintuitive that a prosecutor can more effectively manage information when there is more information available, but the core issue is whether or not the prosecutor is aware of the information, and an integrated criminal justice information system can strengthen this awareness. It will be less convincing, consequently, for a prosecutor to claim that she was ignorant of exculpatory information within an integrated information sharing system. Hence, a prosecutor may end up being more dutiful—and accountable—as information-sharing increases.

---

[234] In *Kyles v. Whitley*, Justice Souter captures this idea in discussing some of the practical problems a prosecutor may face in meeting his or her *Brady* obligations: "In the State's favor it may be said that no one doubts that police investigators sometimes fail to inform a prosecutor of all they know. But neither is there any serious doubt that 'procedures and regulations can be established to carry [the prosecutor's] burden and to insure communication of all relevant information on each case to every lawyer who deals with it.'" 514 U.S. 419, 438 (1995).

C. Evidentiary Privileges

Many people are roughly familiar with traditional privilege rules, such as the attorney-client privilege, the psychotherapist-patient privilege, and the privilege between clergy and their parishioners. Privilege laws are generally designed to protect information from disclosure in litigation or other formal legal proceedings. Privilege, therefore, differs from "confidentiality" laws that require (or permit) agencies to withhold certain information from disclosure regardless of whether any formal proceeding is involved. Most commonly, privilege laws allow an individual to refuse to testify, or to refuse to answer certain questions when under subpoena in a court, regulatory proceeding, legislative hearing, or grand jury.

The majority of conventional privilege laws will not affect information-sharing among criminal justice agencies for one reason: The most common effect of these privilege laws is to enable private parties to withhold information from the government (or other private parties). The common privilege laws may prevent the government from getting certain information in the first instance, but they rarely affect the ability of agencies to use or share that information when it has been legally obtained. On the other hand, there are some rules that fall into the category of privileges—especially official business privileges—that require discussion in this Primer. In any event, a brief review of the overall nature and operation of privilege laws supplies helpful context for information sharing responsibilities.

1. Evidentiary Privileges

Most of the relevant privilege laws appear in the Evidence Code and apply to both civil and criminal cases. Penal Code sections 1054.6 and 1102 are also relevant to criminal cases. Under Penal Code Section 1054.6:

> Neither the defendant nor the prosecuting attorney is required to disclose any materials or information which are "work product," as defined in subdivision (c) of Section 2018 of the Code of Civil Procedure, or which are privileged pursuant to an express statutory provision, or are privileged as provided by the Constitution of the United States.

And Penal Code 1102 states that "the rules of evidence in civil actions are applicable also to criminal actions, except as otherwise provided in this

code."[235]

The result is that the Evidence Code's privilege rules generally apply in criminal cases just as they do in civil cases.[236] These main privileges are:

> (1) self-incrimination[237]; (2) marital communications[238]; (3) attorney-client[239]; (4) clergyman-penitent[240]; (5) psychotherapist-patient[241]; (6) sexual assault counselor-victim[242]; (7) official information[243]; (8) newsperson's privilege[244]; (9) identity of informer[245]; (10) domestic violence counselor-victim[246]; and (11) attorney work product.[247]

Putting aside the unique nature of the privilege against self-incrimination (rooted in the Fifth Amendment to the Constitution), these are typically "communications" privileges designed to protect personal relationships or other interests where the protection of confidentiality outweighs the need for evidence. Privileged information, as a consequence, is formally defined as "a confidential communication between properly related parties and incident to the relation."[248]

---

[235] CAL. PENAL CODE § 1102 (2008). *See also* 4 WITKIN CAL. CRIM. LAW CRIM PROC § 4.2 (2008).

[236]The one key anomaly is that the broad physician-patient privilege applies solely in civil cases, although psychotherapist-patient privilege (covering physicians serving as therapists as well as well as clinical psychologists and licensed clinical social workers) does apply in criminal cases.

[237] CAL. EVID. CODE § 940 (2008).

[238] *Id.* § 980.

[239] *Id.* § 954.

[240] *Id.* § 1033.

[241] *Id.* § 1014.

[242] *Id.* § 1035.8.

[243] *Id.* § 1040 (2008); *see also* CAL. GOV'T CODE 6254(k) (2008).

[244] CAL. EVID. CODE § 1070 (2008).

[245] *Id.* § 1041.

[246] *Id.* § 1037.5.

[247] *Id.* § 915(a).

[248] *Id*. There are four elements that must be present in order for claimant to suppress information under a privilege. A privilege may be asserted if (1) it concerns a communication, (2) the nature of the communication is confidential; (3) the communication occurred properly between related parties as set out in the Evidence Code; and (4) the communication is incident to the parties' relationship

A privilege encompasses three rights: (1) the personal right to refuse to disclose the privileged information; (2) the right to prevent third parties from making disclosure; and (3) the right to prevent opposing counsel and the judge from commenting on the exercise of a privilege.[249] These privileges typically apply in any proceeding in which testimony can be compelled.[250] But privileges also apply outside formal legal proceedings. If a privilege permits a person to withhold information when required by a lawful subpoena or court order, then it follows that the same party can withhold information upon any request (formal or informal) made outside the scope of legal proceedings.

The privilege to withhold information, nevertheless, may be waived. If a privileged party chooses to disclose the information, then the privilege is nullified. Moreover, some disclosures by a party may waive the privilege even if the party did not intend to waive, or even realize she was waiving.

If an agency seeks information from a privileged party, it may seek a deliberate and express waiver; although, by definition, it normally has no power to compel waiver. Sometimes an agency may end up accessing privileged information because the privileged party has unintentionally waived. Generally, one cannot *selectively* waive a privilege. If a privileged party discloses the information to some third party not covered by the privilege (i.e., a client discloses an attorney-client communication to someone not his lawyer and not directly associated with the lawyer), then the privilege disappears, and another third party can likely compel disclosure when seeking it in a formal proceeding. And, finally, a privileged person who discloses information to a third party outside the criminal justice system has probably waived the right to resist a formal request from a criminal justice agency that otherwise has a legal basis for

---

(i.e., person is seeking psychotherapy or legal advice). In general, communication consists of 'both oral and written statements intended to convey meaning to the hearer and reader.' A communication is confidential if the holder of the privilege intends for the information to remain private or secret and if the communication is not made in the presence of a third party who is not present to further the interest of the client.

[249] 1-10 CALIFORNIA EVIDENTIARY FOUNDATIONS B (2008).

[250] California Evidence Code Section 901 defines proceedings as "any action, hearing, investigation, inquest, or inquiry (whether conducted by a court, administrative agency, hearing officer, arbitrator, legislative body, or any other person authorized by law) in which, pursuant to law, testimony can be compelled to be given. CAL. EVID. CODE § 901 (2008).

the request.

Thus, most privileges will operate to deny government agencies access to covered information (absent waiver). The communication privileges enumerated above will rarely operate to give the public agency itself a privilege to withhold information it controls. The attorney client-privilege, however, does also belong to government officials. An agency or official who is a "client" of a government lawyer has the traditional privilege with respect to confidential client-lawyer communications, as well as the closely allied privilege for attorney "work product." This latter privilege is really a subset of the broader privilege category that applies to government-held information, the so-called official business privilege, to which we now turn.

2. Official Information Privilege as a Barrier to Information Sharing Among Criminal Justice Agencies

The official information privilege is the only way a public entity may refuse to disclose information that it or the legislature has deemed confidential (e.g., California Public Records Act). Official information is defined as "information acquired in confidence by a public employee in the course of his or her duty and not open, or officially disclosed, to the public prior to the time the claim of privilege is made."[251] A public entity can elect not to disclose or share official information and prevent a third party from disclosing official information if one of the following conditions is met: "(1) disclosure of the information is forbidden by a federal or a California statute or (2) disclosure is against the public interest (i.e., a court must weigh the need for confidentiality against the need for disclosure in the interest of justice)."[252]

Penal Code Sections 1040(b)(1)-(2) essentially creates two types of official information privileges. There is an absolute privilege against disclosure of official information (Penal Code Section 1040(b)(1)) and there is a conditional privilege against disclosure of official information (Penal Code Section 1040(b)(2)) that covers all information that is not privileged under Penal Code Section 1040(b)(1). If the privilege is claimed by an eligible public employee on behalf of the public entity and the disclosure is prohibited by an act of Congress or by a California statute, the public entity has an *absolute* privilege to refuse to disclose the official information. If the

[251] CAL. EVID. CODE § 1040(A) (2008).
[252] *Id.* § 1040(B)(1)-(2).

privilege is claimed by an eligible public employee on behalf of the public entity and the court determines the disclosure is against the public interest, the public entity has a conditional privilege to refuse to disclose the official information.[253]

There are two qualifications to Penal Code Sections 1040(b)(1)-(2).[254] Similar to qualifications and waiver rules for other types of privileges, "official information is neither conditionally nor absolutely privileged if it was not acquired in confidence or if it was officially disclosed to the public prior to the time the claim of privilege was made.'[255] In addition, a public entity may not claim a conditional privilege if an employee, who is authorized to claim the privilege, already consented to disclosure.

This privilege interacts in important ways with Chapter 2 (Criminal Offender Record Information) of Title 3 of Part 4 of the California Penal Code, which creates a strong foundation for integrated criminal justice information systems and, more generally, formalized information sharing among actors in the criminal justice system.[256] Penal Code Section 13100, in part, recognizes the need for improved access to and sharing of information across criminal justice agencies.[257] In particular, Penal Code Section 13100(a) explains that "the criminal justice agencies in this state require, for the performance of their official duties, accurate and reasonably complete offender record information."[258] Penal Code 13100(e) states that "the recording, reporting, storage, analysis, and dissemination of criminal offender information in this state must be made more uniform and efficient, and better controlled and coordinated."[259]

Penal Code Section 13300(1) authorizes local criminal justice

---

[253] *Id*.

[254] 2 WITKIN CAL. EVID. WITNESSES § 247 (2008).

[255] CALIFORNIA FORMS OF PLEADING AND PRACTICE—ANNOTATED § 191.81 (2008) (citing CAL. EVID. CODE § 1040(a)).

[256] CAL. PENAL CODE § 11105(A)-(S) (2008).

[257] Criminal justice agencies are defined under Penal Code Section 13101(a)-(b) as "those agencies at all levels of government which perform as their principle functions, activities which either: (a) relate to the apprehension, prosecution, adjudication, incarceration, or correction of criminal offenders; or (b) relate to the collection, storage, dissemination or usage of criminal offender record information." CAL. PENAL CODE § 13101(A)-(B) (2008).

[258] CAL. PENAL CODE § 13100(A) (2008).

[259] *Id.* § 13100(E).

agencies to compile and share selected "local summary criminal history information" pertaining to "the identification and criminal history of any person, such as name, date of birth, physical description, dates of arrest, arresting agencies and booking numbers, charges, dispositions, and similar data about a former criminal offender."[260] A local criminal justice agency is permitted to share local summary criminal history information with selected parties, including public defenders and attorneys of record, district attorneys, courts, probation officers, and the former criminal offender.[261]

But while Penal Code Section 13300 et seq. provides a basic statutory foundation for information sharing among criminal justice agencies, there are statutory limits on the information that the criminal justice agencies are permitted to share, and which can trigger the absolute privilege discussed above. Namely, local criminal justice agencies may only share summary information and may not share information derived from independent investigations or intelligence information.[262] Penal Code Section 13102, moreover, provides that criminal record information compiled by criminal justice agencies must not include information such as intelligence, analytical, and investigative reports or files.[263]

In effect, the statutory provisions that address permitted information sharing among local criminal justice agencies suggest that the official information privilege poses the most significant barrier to more effective information sharing. Assuming that most criminal justice agencies have sufficient access to summary criminal history, as limited by statute and court decisions, and that summary criminal information is accurately maintained, criminal justice agencies still do not have formal access to "contemporaneous" information about offenders. Given that the official information privilege generally prevents the disclosure of investigative files, most criminal justice agencies would benefit from formalized access to this information possessed by other law enforcement agencies.[264]

3. The Potential Impact of Official Information Privileges on Information Sharing

Criminal justice agencies are likely to invoke their official information privileges when they relate to "contemporary" information,

---

[260] *Id.* § 13300(A)(1).
[261] *Id.* § 13300(3)(B)(1)-(16).
[262] *Id.* § 13300(A)(2).
[263] *Id.* § 13102.
[264] 2 WITKIN CAL. EVID. WITNESSES § 264 (2008).

information related to an ongoing investigation or pending adjudicatory proceeding. Those agencies may prefer to self-report and share summary information under Penal Code section 13300(1), thereby avoiding the exposure of sensitive investigative information – a concern raised by Penal Code section 13102 – if a defendant or third party seeks broader discovery.

In some ways, it is best to think of the official information privilege as a type of work-product privilege (at least in the summary versus contemporary information comparison), with Section 13300 allowing for information that is fundamentally factual to be shared. By no means perfect, the analogy speaks to the idea that criminal justice agencies have an interest in keeping their investigative processes and confidential sources private, as the privilege protects information (i.e., underlying methods and notes of investigators) that is not included in a summary report.

The official information privilege, therefore, poses a "barrier" to criminal justice information systems, as it undoubtedly prevents some information from being included in an integrated database. That impact, however, is true of all privileges. Thus, if the goal of a criminal justice system is simply to formalize communication among criminal justice actors, then privileges pose no real "barrier" to the effectiveness of that mission. In this regard, formal information-sharing networks would complement the informal networks that already exist and, at the least, give criminal justice actors a centralized source of information.

Consequently, the real value of a criminal justice information system rests not in its comprehensiveness, but rather in its ability to facilitate communication and interagency coordination. As long as actors are aware (and they likely are), that the information documented in an information system is not entirely representative of the information that participating criminal justice actors either have or have access to (based on their relationship to the privilege holder), then the privileges do not interfere with effective data sharing.

In sum, privileges don't "matter" to information sharing systems in the sense that privileges are not new and have always posed a barrier. These systems remain important, moreover, because they can change the regular means of communication and coordination between agencies (i.e., formal, searchable databases versus unconnected conversations and personal contacts), not because they guarantee the information in their databases is fully comprehensive.

4. Waiver of Privileges: Consent to Disclose as a Mechanism to Facilitate Information Sharing Between Criminal Justice Agencies

The holder of the privilege has the right to prevent another person from disclosing privileged information. Assuming that the privilege holder has not waived the privilege implicitly, and that an applicable exception to a privilege does not apply, criminal justice agencies must get permission (as third party representatives) to integrate and share that privileged information.[265]

Evidence Code Section 912(a) provides that the holder of a privilege waives a claim to a privileges if he or she has voluntarily "disclosed a significant part of the communication or has consented to disclosure made by anyone."[266] Section 912(a) further explains that "consent to disclosure is manifested by any statement or other conduct of the holder of the privilege indicating consent to the disclosure, including failure to claim the privilege in any proceeding in which the holder has the legal standing and opportunity to claim the privilege."[267] Some disclosures do not amount to a waiver of the privilege if the disclosure itself is privileged (i.e., privileges may be layered).[268]

What if the criminal justice agency possesses the privilege (i.e., official information)? In this situation, a criminal justice agency may be reluctant to waive its privilege and participate in an information sharing network, particularly if an unaligned party (e.g., public defenders and general members of the public) would gain unfettered access to information. This is particularly important given the theory that privileges cannot be selectively waived.[269] As a procedural matter, a third party criminal justice agency that waives the privilege would no longer be considered a third party once it participates in an integrated information system. The information possessed by the agency would no longer be subject to a *subpoena duces tecum*. Instead, the opposing counsel would simply have to demonstrate that the holder or representative of the holder of the privilege waived the privilege.[270]

---

[265] *See generally* 16-191 CALIFORNIA FORMS OF PLEADING AND PRACTICE—ANNOTATED § 191.15 (2008) (discussing waiver of privileges generally).

[266] *Id.*

[267] *Id.*

[268] CAL. EVID. CODE § 912(D) (2008).

[269] *See* 2 WITKIN CAL. EVID. WITNESSES § 300 (2008) (discussing agency's voluntary disclosure of privileged official information).

[270] CAL. EVID. CODE § 912(A) (2008).

In effect, the information would remain sensitive, but it would technically not be confidential. A party that engages in interagency information sharing could still protect its interest in confidentiality by filing a motion to limit or deny the requested discovery. But the party attempting to limit the disclosure of information would have a less compelling argument for confidentiality since it already waived associated privileges. Therefore, even if the party gets an in-camera review of the evidence in question, it may ultimately be forced to the disclose information.

Another potential impediment and concern regarding waiver of privileges by certain criminal justice agencies is that the privilege may not be waivable. For example, government entities subject to the disclosure requirements and exemptions of the California Public Record Act, discussed above, may not disclose information that is prohibited by law.[271] There may be an overriding state public interest in non-disclosure of certain privileged information that prohibits local agencies from disclosing and sharing public records that are exempt from disclosure.[272]

VII. LIABILITY

Law enforcement officials have expressed concern that disclosing information, or relying on inaccurate information, might expose them to personal liability. This section deals with departmental and individual liability that might result from misuse of information or inaccurate information. The bottom line is that fears of liability are overstated. Provided that agencies follow safeguards—safeguards they are already required to follow under CLETS guidelines—they should not be exposed to any liability. If there are rogue employees who deliberately violate policies or otherwise misuse information, the liability will attach to them personally. But if agencies use data in a reasonable fashion, in the ordinary course of business, it is unlikely that they can be sued for damages.

Before turning to specific cases, it is useful to discuss the field of tort law and §1983 law more generally. Tort law concerns the civil wrongdoing of one party as against another; this is generally what people mean when they talk about suing someone for something. Torts can be intentional or

---

[271] CAL. GOV'T CODE § 6254 (2008) ("Nothing in this section prevents an agency from opening its records concerning the administration of the agency to public inspection, unless disclosure is otherwise prohibited by law.").

[272] *See, e.g.*, Younger v. Berkeley City Council, 45 Cal. App. 3d 825 (Ct. App. 1975).

unintentional, and they can result in injunctive relief (being forced to do or not to do something) or damages (usually money). Parties can be agencies and organizations, and they can also be individuals. §1983 liability comes from a federal statute prohibiting officials from violating individuals' constitutional rights.

For tort, one primary question is who can be sued. In the work environment, the key question is when an employer is liable for the actions of its employee—for example, when a police department is responsible for the actions of an individual officer. This type of liability is known as *respondeat superior* liability. Generally, an employer is only responsible for the actions of its employee when that employee is acting within the scope of employment. If an employee is not on the clock, or not doing the ordinary business for which he or she was hired, and/or not abiding by company policy, then the employer is not responsible. So a police officer on the beat would be in the scope of employment, but an out-of-uniform police officer on vacation would not be. Many tort claims against agencies could be resolved by this doctrine, provided the individuals were not acting within their scope of employment.

The second thing to consider is who pays damages. Individuals are often, as a matter of their employment contracts, indemnified against suits. This means that, generally, individuals need not pay to defend themselves against suits arising from their employment, nor do they need to pay damages should they lose. Indemnification is a near universal feature of law enforcement contracts and covers both ordinary torts and §1983 claims.

Section A of this part concerns the tort claims of defamation and invasion of privacy, concluding that the risks of being successfully sued under either theory is remote. Section B looks at individual suits under § 1983. Section C looks at the remote possibility that an individual might grossly misuse information—say, selling access to a database—concluding that in such cases it is unlikely that an agency will be held responsible for such actions. Finally, Section D considers whether there might be proprietary intellectual property claims made against those who use data.

A. Tort Claims for Defamation and Invasion of Privacy

The bulk of this Primer addresses a number of very specific and highly technical rules governing disclosure of criminal justice information, most of them arising under state and federal statutes regulating public agencies. An equally important arena, however, are the two traditional legal

doctrines of defamation and invasion of privacy. Perhaps the most common worry for public officials handling personal information is the possibility of a lawsuit under one of these grounds. A summary of the basic doctrines in these areas, however, should provide reassurance that this concern is greatly exaggerated. The criteria for defamation and invasion of privacy claims—and the special immunities accorded public officials under these doctrines—make it very unlikely that such lawsuits will be filed, and even less likely that they will succeed.

1. Defamation

Defamation is the utterance of a false statement about an individual that damages that person's reputation in some material way. A statement can only be defamatory if it is about a factually verifiable matter, not if it is an expression of subjective opinion, however negative that opinion is. The false factual statement must cast the individual in a bad light as understood by established and customary moral and social standards. Defamation is called libel if it is written or published in some printed form; it is called slander if it is expressed orally.

A criminal justice agency can generally protect itself from defamation claims by implementing careful policies that inhibit the unintentional republication of data outside the agency. Moreover, if an alleged defamer is a government official and the statement that would otherwise qualify as defamatory is made in the course of designated duties, the official enjoys special exemptions from personal liability.

In California, a statement made or released by a public official "in the proper discharge of an official duty" is absolutely privileged and thus cannot support a defamation claim, even if the statement is erroneous.[273] For instance, in *Kilgore v. Younger*, a prosecutor erroneously included the plaintiff's name in a press release naming persons suspected of organized crime activity. The Supreme Court of California held that the press release, though improper, was within the scope of the prosecutor's legitimate duties and thus was privileged.[274]

---

[273] CAL. CIV. CODE § 47 (2009). One test courts have used to determine whether an allegedly defamatory statement was made in the exercise of an official function is whether the communication "was an appropriate exercise of the discretion which an officer of that rank must possess if the public service is to function effectively." *Barr v. Matteo*, 360 U.S. 564, 574-75 (1959).

[274] *Kilgore v. Younger*, 30 Cal. 3d 770, 779-81 (1982). Similarly, in *Kim v. Walker*, 208 Cal. App. 3d 375 (Ct. App. 1989), the court determined that statements by a parole agent, a deputy county counsel, and a policeman that allegedly defamed the plaintiff by

A plaintiff alleging defamation against a criminal justice official can overcome this privilege by meeting one of two tests. The first test requires the plaintiff to show that the challenged action was not part of the official's designated functions. This test establishes a high hurdle, as courts construe the term "appropriate exercise of the [official's] discretion" broadly.[275] The second test requires the plaintiff to show that the defamatory statement was made with "actual malice." This would require the plaintiff to demonstrate that the official uttered the statement with "hatred or ill will toward the plaintiff" or that the official, lacking any reasonable grounds for belief in the truth of the statement, uttered it in "reckless disregard" of its falsehood.[276] In the area of criminal justice information, the worst that a plaintiff could normally allege is that an official was careless in disseminating a falsehood; thus, in the absence of hatred or ill will, the actual malice test is almost impossible to meet in the criminal justice context.

Furthermore, in the very unlikely event of a viable defamation suit against a public official, the First Amendment limits the amount of damages the official can be required to pay.[277] In earlier eras, juries were allowed to *presume* that harm had occurred and make awards without specific proof of damages. But under contemporary First Amendment law, in cases where (1) the challenged utterance related to a matter of public concern and (2) the alleged defamer did not know the statement was false, monetary recovery is limited to "actual" damages—*provable* harm to reputation and emotional harm.[278] Because criminal justice matters are often of public concern, the actual damages rule significantly limits the exposure of government agencies to tort actions.

Other state law privileges overlap with and supplement this official immunity to provide criminal justice officials even stronger protection against defamation suits. First, allegedly defamatory statements uttered during the course of formal litigation are absolutely privileged.[279] Second, police and correctional officers are immunized against *common law* tort suits by arrested or imprisoned individuals except in narrow exceptions

---

stating that he had molested his daughter were privileged.

[275] *Copp v. Paxton*, 45 Cal. App. 4th 829, 841, 844 (Ct. App. 1996).

[276] *Roemer v. Retail Credit Co.*, 44 Cal. App. 3d 926, 936 (Ct. App. 1975).

[277] Dan B. Dobbs, THE LAW OF TORTS, § 422 (2000).

[278] *Id.*

[279] *Id.* at § 412.

(like vehicular torts and physical assault) that do not include defamation.[280]

Furthermore, federal government officials are protected against defamation-related causes of action by the Federal Tort Claims Act (FTCA), a federal statute that immunizes all federal employees acting within the scope of their employment from tort liability including defamation.[281]

Finally, the most powerful statutory remedy available to individuals suing state officials for unconstitutional actions is of no avail in defamation suits. That statute, 42 U.S.C. § 1983, allows individuals to sue state or local officials who have violated their federal (usually constitutional) rights. Thus, an individual who claims to be the victim of an unconstitutional search and seizure or a prisoner who alleges abusive conditions in violation of the Eighth Amendment can sue under § 1983 (although even then, individual officials enjoy a "qualified immunity" if their actions were based on a reasonable, but erroneous, belief that they were lawful[282]). However, there is no federal constitutional right not to be defamed; protection of reputation is a right developed by common law tradition and enjoys no constitutional status.[283] Consequently, § 1983 is not an available remedy for defamation claims.

2. Invasion of Privacy

In contrast to defamation, invasion of privacy involves statements that are concededly true. Moreover, a plaintiff claiming invasion of privacy need not allege that the statements complained of harmed his or her reputation. In invasion of privacy actions, the alleged harm is that public disclosure of information violated the plaintiff's right to keep certain intimate personal facts confidential.

The U.S. Supreme Court has recognized a constitutional right of privacy with respect to *some* aspects of a person's private life—namely intimate matters about marriage, family, or sexuality—that are protected from excessive government regulation. But the federal Constitution does not recognize a broader *general* right to keep private matters from public

---

[280] CAL. GOV'T CODE § 844 *et seq.* (2008). Of course, immunity from *common law* tort suits does not protect police and correctional officers from *constitutional* claims brought under 42 U.S.C. § 1983, which is in Part B, *infra*.

[281] *See* 28 U.S.C. S 2680(h) (2010).

[282] Qualified immunity in § 1983 actions is addressed in Part B, *infra*.

[283] *See Paul v. Davis*, 424 U.S. 693 (1976).

disclosure. Rather, the source of this right is in state law.

The California Constitution explicitly provides a right to privacy,[284] the violation of which can be the basis for a civil lawsuit. An individual has a cause of action for violation of this right if she can establish a legally protected privacy interest, a reasonable expectation of privacy in the circumstances, and conduct that constitutes a serious invasion of privacy.[285] In determining whether the right has been breached, courts and juries look to factors including the likelihood of serious harm, particularly to the emotional sensibilities of the victim, the alleged intruder's motives and objectives, and the absence of countervailing interests from competing social norms, rendering an individual's conduct offensive. Countervailing interests include a legitimate public interest in (1) exposing otherwise private information or behavior and (2) prosecuting serious crimes.[286] This last factor is a significant limitation on invasion of privacy lawsuits against criminal justice actors, since otherwise non-privileged facts contained in criminal justice records are likely to satisfy this criterion.

On the other hand, if a criminal justice official asserts a sufficient countervailing interest, the plaintiff gets a chance to rebut that countervailing interest by showing there are feasible and effective alternatives to the defendant's conduct that have a less severe impact on the plaintiff's privacy interest. But even this is a high hurdle for the plaintiff:

> For example, if intrusion is limited and confidential information is carefully shielded from disclosure except to those who have a legitimate need to know, privacy concerns are assuaged. On the other hand, if sensitive information is gathered and feasible safeguards are slipshod or nonexistent, or if defendant's legitimate objectives can be readily accomplished by alternative means having little or no impact on privacy interests, the prospects of actionable invasion of privacy is enhanced.[287]

Thus, a criminal justice official who can demonstrate that a privacy intrusion was limited and that confidential information has been shielded from disclosure other than to those who have a legitimate need to know

---

[284] CAL. CONST. art. I, § 1.
[285] *See* 6A CAL. JUR. 3d, *Assault and Other Willful Torts*, § 120, *et seq.* (2010)
[286] *See Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1 (1994).
[287] *Id*.

should have little trouble defending him or herself against an invasion of privacy claim, even if alternatives to the invasion existed.

Finally, other common law doctrines make an invasion of privacy suit even less of a concern for public officials. First, if the information is contained in a form that already constitutes a public record (such as facts contained in most non-juvenile court records), then disseminating the information more widely cannot, by definition, violate the right to privacy.[288] Statements made during the course of litigation are, as with defamation suits, absolutely privileged and thus cannot serve as the basis for a tort suit.[289] Moreover, the privilege for discharge of official duties, discussed earlier, also applies in privacy suits, and—as with defamation—overcoming immunity in privacy cases requires the plaintiff to allege that the disclosure did not fall within the broad description of an official's duties or that the disclosure was motivated by "actual malice."

The bottom line for invasion of privacy claims—like that defamation claims—is that common law doctrines leave ample room for effective and efficient information sharing among criminal justice officials, so long as the sharing has a legitimate criminal justice purpose.

B. Individual Liability Under § 1983

Police employees who rely on inaccurate data should not be concerned about civil lawsuits brought under 42 U.S.C. § 1983, the statute permitting individuals to sue for violations of federally protected rights. In most cases, qualified immunity will protect the police officers against a § 1983 claim, and where the error is a result of mere negligence, no Due Process violation will arise. Senior law enforcement officials are not likely to face liability: *respondeat superior*, the doctrine allowing employers to be held responsible for their employees' actions, does not apply to suits brought under § 1983. Liability may occur only where they exhibit bad faith in the form of "deliberate indifference"—i.e., where they knew it was certain or highly likely that they were relying on inaccurate data.

First, qualified immunity shields "government officials . . . from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person

---

[288] *See* 6A CAL. JUR. 3d, *supra* n. 13. What constitutes a "public record" is addressed in Part V.A, *supra*.

[289] *See Jacob B. v. County of Shasta*, 40 Cal. 4th 948 (2007).

would have known."[290] In other words, even if a government official violates an individual's rights, qualified immunity will shield her from liability if she could not reasonably have known she was violating those rights. Qualified immunity aims to protect government officials who reasonably believe that the alleged unlawful act was lawful in light of clearly established law and the factual information possessed at the time.[291] For example, when a police officer relies on a search or arrest warrant premised on data which, unbeknownst to him, is inaccurate (as in *Herring* and *Evans*), he will likely be granted immunity because a reasonable officer in his position "would not have known there was no constitutional basis for" the arrest or search.[292] Even if a police employee makes an initial mistake in an arrest warrant database that leads to an unlawful search (as in *Herring*), that employee will not be subject to § 1983 sanctions, so long as her mistake did not *intentionally* lead to the arrest.[293] That is, no liability will result if, in making the negligent errors, the police officer did not intend to violate the individual's constitutional rights.

Second, a suspect who suffers a Fourth Amendment violation (i.e., a search or seizure violation) as a result of a police officer's reliance on inaccurate data will not succeed in bringing a cause of action where the violation was the result of mere negligence.[294] If, however, a system contains widespread errors, the violation may rise to the level of "deliberate indifference" to the suspect's constitutional rights, which could enable the suspect to prevail against an individual police officer on a Due Process claim.[295] Thus, police departments should establish reliable warrant systems to avoid potential liability stemming from a finding of "deliberate indifference."

Third, senior law enforcement officials cannot be held liable for their subordinates' constitutional violations because *respondeat superior* does not apply to § 1983 actions.[296] If, however, the suspect can show that

---

[290] Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982).

[291] *See* Saucier v. Katz, 533 U.S. 194, 206-09 (2001).

[292] Brief for Am. Civil Liberties Union and the ACLU of Alabama as Amici Curiae Supporting Petitioner, Herring v. United States, 129 S. Ct. 695 (2009) (No. 07-513).

[293] *See* Brower v. County of Inyo, 489 U.S. 593, 596-97 (1989) ("[A] Fourth Amendment [violation occurs] . . . only when there is a governmental termination of freedom of movement *through means intentionally applied*.").

[294] Daniels v. Williams, 474 U.S. 327, 333-35 (1986).

[295] *See* County of Sacramento v. Lewis, 523 U.S. 833, 853-854 (1998).

[296] Monell v. Dep't of Soc. Serv., 436 U.S. 658, 691 (1978).

an official policy or practice, or a failure to train that amounts to deliberate indifference caused the violation, the *county* may be held liable.[297] Note, however, that courts typically view police departments enforcing criminal law as arms of the state, thereby shielding the county from liability under the state's Eleventh Amendment immunity.[298] Still, the potential civil liability and evidentiary consequences of reckless data keeping should caution police departments to establish and maintain reliable databases.

Finally, a suspect who suffers a constitutional violation will almost certainly fail in efforts to gain injunctive relief under § 1983. The suspect can gain injunctive relief only if he can "establish a real and immediate threat" that he will suffer the same constitutional violation again.[299] In *Herring*, for example, the petitioner would need to show that "he would again be the subject of an arrest warrant that was later revoked but not removed from a computer database, and that this outdated information would again become the basis for his subsequent unconstitutional arrest."[300] This would be a nearly impossible showing to make.

The lack of a process for reporting inaccurate personal data may, in certain circumstances, however, leave open the possibility of a lawsuit. In particular, false public records may give rise to tort suits for constitutional violations (e.g., under § 1983) when the claim involves more than mere defamation or violation of privacy, and implicates another constitutional right. Most notably, a federal appeals court allowed two parents to proceed with a suit against Los Angeles County after they were placed on California's Child Abuse Central Index.[301] The database was made widely available, and no procedure existed to petition to have erroneously included names removed from the list.[302] The court found that the lack of any recourse for erroneous records violated the Due Process guarantees of the 14th Amendment.[303] The court dismissed the case against the individual officers named in the suit because they had acted in official capacities, but the court found that the county could be held liable and remanded the case

---

[297] *Id.* at 694.

[298] McMillan v. Monroe County, 520 U.S. 781, 793 (1997).

[299] City of Los Angeles v. Lyons, 461 U.S. 95, 105 (1983).

[300] Brief for Am. Civil Liberties Union and the ACLU of Alabama as Amici Curiae Supporting Petitioner at 12, Herring v. United States, 129 S. Ct. 695 (2009) (No. 07-513).

[301] Humphries v. County of Los Angeles, 554 F.3d 1170 (9th Cir. 2009).

[302] *Id*. at 1179.

[303] *Id*. at 1175.

for further trial.[304] By contrast, a federal appeals court dismissed all § 1983 claims by a woman placed on the federal no-fly list, but it did allow some claims to receive further hearing, including a challenge under the Administrative Procedure Act, which allows individuals to file a lawsuit to enjoin illegal actions by a federal agency.[305]

To avoid the possibility of legal liability under § 1983, agencies should consider implementing procedures for individuals to check their records and petition for the correction of inaccurate data. Though the unreviewable inclusion of inaccurate data may not rise to the level of violating an individual's constitutional rights, inadequate procedures for redress can help a plaintiff move from a mere right-to-privacy claim (which will usually be dismissed because of governmental privileges) to a § 1983 claim.

C. Misuse of Information

Deliberate and gross misuse of information leads to individual liability alone. Gross misuse will not tend to make agencies and employers liable, simply because such actions are not reasonably foreseeable. When harms cannot be foreseen, there is nothing an employer could have done to prevent the harm from occurring, and thus nothing it needs to do to make the harmed party whole.

Consider this example. In 2001, a former Drug Enforcement Administration (DEA) agent was arrested after being caught selling criminal justice data from CLETS and other national databases to private investigators.[306] The DEA agent, Emilio Calatayud, was charged with several criminal offenses: illegally accessing law-enforcement computer systems, wire fraud, and bribery.[307] There was, however, no civil liability in this case. In order to make a claim that the DEA was responsible, a plaintiff would have to show that Calatayud acted according to official policy (which he clearly didn't), or that his supervisors knew (or should

---

[304] *Id*. at 1203.

[305] Ibrahim v. Dep't of Homeland Sec., 538 F.3d 1250 (9th Cir. 2008); *see also* 5 U.S.C. § 702 (2009).

[306] *DEA Data Theft Raises Privacy Concerns*, CNET NEWS, Jan. 24, 2001, http://news.cnet.com/DEA-data-theft-raises-privacy-concerns/2009-1023_3-251426.html.

[307] *Id*.; *see also* Press Release, United States Department of Justice, Former DEA Agent Pleads Guilty to Bribery, Tax Charges (Aug. 1, 2002), *available at* http://www.usdoj.gov/tax/usaopress/2002/txdv02DOJ456.html.

have known) that he was engaged in this behavior and they deliberately did nothing to stop it. Absent that showing, the liability (both criminal and civil) stops with him.

Taking a darker hypothetical, albeit one that this author has heard several times from concerned law enforcement officials, suppose a rogue officer took someone's address from a proprietary database and then went and shot them. Would the agency be liable? In a word, no. Clearly this behavior would be outside the scope of employment. Clearly it would not have been official policy. Clearly the behavior was illegal and would be dealt with in the criminal justice system. It is, of course, true that anyone can file a suit against anyone, but absent a showing that the employer knew or should have known that this was happening (or going to happen), and that the employer then did nothing to stop it, there is simply no way that the claim would survive immediate dismissal. Tort liability does not extend to everyone any time something goes wrong. It only extends to foreseeable harms that cause damages, where someone who had a duty to prevent the harm breached that duty. There is no duty to guard against one-in-a-million harms that couldn't possibly be foreseen.

D. Criminal Justice Databases and Intellectual Property

Government agencies sometimes refer to holding a "copyright" or "ownership" in criminal justice data.[308] This language evokes concepts of intellectual property rights, but such rights do not appropriately apply to criminal justice data. When agencies claim "ownership" and "copyright" in data, therefore, they are most likely invoking the security and privacy concerns discussed above, *not intellectual property concerns.* Agencies

[308] *See, e.g.*, City of Concord, *General Conditions*, *in* APPROVAL OF A THREE YEAR INTERAGENCY AGREEMENT BETWEEN CITY OF CONCORD AND CONTRA COSTA SHERIFF'S OFFICE FOR CLETS LEVEL II ACCESS, CONTRA COSTA COUNTY PURCHASE OF SERVICES IN A TOTAL AMOUNT OF $22,600 8, 12 (June 23, 2008), *available at* www.ci.concord.ca.us/citygov/agendas/council/2008/06-23-08/3l.pdf ("Copyrights and Rights in Data: Contractor shall not publish or transfer any materials produced or resulting from activities supported by this agreement without the express written consent of the County Administrator."); INTERGOVERNMENTAL AGREEMENT BETWEEN AUTOMATIC RECORDS RETRIEVAL AND ELECTRONIC SHARING TECHNOLOGY (A.R.R.E.S.T.) AND LOS ANGELES COUNTY SHERIFF'S DEPARTMENT 3 (April 20, 2009), *available at* http://www.cdaid.org/mod/userpage/images/GSpacket042709.pdf (Section III discusses "Information Ownership," providing that "Each Agency Party retains control of all information it provides to COPLINK").

should not resort to intellectual property terminology as shorthand for security concerns; doing so confuses security issues with misplaced fears about violating intellectual property rights. Officials should be skeptical of other agencies' arguments for nondisclosure if those arguments are couched in the language of property ownership.

Intellectual property law allows for the copyright protection of original works that are independently created by an author with some element of creativity.[309] The focus of copyright law is on the *form of original expression*, not on empirical facts or abstract ideas that are the content or subject of the thing expressed. In *Feist Publications, Inc. v. Rural Telephone Services Co.*, the United States Supreme Court considered whether data compilations, such as a database, could be protected by copyright.[310] The court affirmed the principle that facts cannot be copyrighted, because they "do not owe their origin to an act of authorship,"[311] but suggested that, "[f]actual compilations . . . may possess the requisite originality."[312] Thus, although criminal justice facts, such as an arrest record or court disposition, are not themselves copyrightable, criminal justice databases that compile factual data may be copyrightable if the compiler selects facts independently and with a "minimal degree of creativity."[313]

Even if some databases are copyrightable in theory, Congress can choose to deny them copyright protection under statutory law. Congress has, for example, explicitly denied copyright protection to works by the *federal government*.[314] With state databases, the legal situation is more complicated. Congress has not categorically denied copyright protection to works of state governments. Thus, if compilations of data by state governments meet *Feist*'s minimal creativity requirement, they can presumptively enjoy copyright protection. Thus, *state law* must be consulted to determine where federal copyright law applies.

In the recent case of *County of Santa Clara v. Superior Court of Santa Clara County*, the County asserted a copyright of its geographic information system (GIS) basemap, refusing to grant a public records

---

[309] 17 U.S.C. § 101 et seq. (2009).
[310] 499 U.S. 340, 345 (1991).
[311] *Id.* at 347.
[312] *Id.* at 348.
[313] *Id.*
[314] 17 U.S.C. § 105.

request to release its mapping data without an end-user restriction.[315] The court held that the California Public Records Act (CPRA) did not explicitly provide copyright protection to public records.[316] Instead, it held that end-user restrictions were "incompatible with the purpose and operation of the CPRA."[317] In the court's view, allowing Santa Clara "to place extra-statutory restrictions" on its records would "undercut" the CPRA's goal to "increase freedom of information by giving members of the public access to information."[318] Although the county may have a copyright to its computer software and source code, as explicitly granted by the CPRA in § 6254.9(a), the court reemphasized the principle that for public records, "restrictions on disclosure are narrowly construed."[319]

It is highly unlikely that criminal justice databases would be found copyrightable, although no court in California has addressed this question directly. And while some criminal justice data (such as criminal history information) is exempt from the CPRA public disclosure requirements because of confidentiality and privacy concerns,[320] criminal justice records are still generally defined as public records, and their exemption from disclosure is unlikely to change the reasoning in *Santa Clara* – absent statutory authority for copyright, a state's claim of copyright to criminal justice data would violate the disclosure policy of the CPRA.[321] Even if the CPRA did not prohibit the state from asserting a copyright to its criminal justice database, the databases are unlikely to possess even the low threshold of requisite creativity established by *Feist*: criminal justice databases like CLETS are mandated by statute and governed by the regulations discussed above, so the compilation of criminal data is not made independently or creatively.

What effect does intellectual property law have, then, on data sharing between criminal justice agencies? The answer is probably none whatsoever, other than protections for the database source code. Any assertion by an agency of an intellectual property right, or "ownership,"

---

[315] 89 Cal. Rptr. 3d 374, 382 (Ct. App. 2009).
[316] *Id.*
[317] *Id.* at 399-400.
[318] *Id.* at 400.
[319] *Id.* at 397.
[320] CAL. GOV'T CODE § 6254(f) (2009).
[321] County of Santa Clara v. Superior Court, 89 Cal. Rptr. 3d 374, 398 (Ct. App. 2009) (discussing CAL. EDUC. CODE § 1044 and CAL. HEALTH & SAFETY CODE § 25201.11(a), which granted copyrights to the state Board of Education and the Department of Toxic Substances Control, respectively).

over criminal justice data would not be enforceable. Although agencies may worry about who "owns" what data, the issue of ownership is not important because agencies cannot enforce an intellectual property right in public records. Instead, what is important (and what agencies are likely trying to express by using language of "ownership") are issues of security and privacy related to data use and secondary dissemination.[322]

CONCLUSION

This Primer has aimed to clear up some common misunderstandings about the legal regime, most notably that data sharing somehow requires agencies to enter uncharted territory. While there are some novel issues that data integration presents—and, as stated earlier, individuals should not rely on this as legal advice but should, instead, consult attorneys before enacting new policies—by and large, data integration does not lead to a significantly larger exposure to regulatory or statutory liability. Criminal justice officials have a number of technical and data is one tool among many, but it can help criminal justice agencies do their jobs more accurately and more efficiently. State and federal laws provide few obstacles towards greater data integration among California's state and local criminal justice agencies. Of course, there are many organizational and technological issues to be worked out, but provided they are, one hopes that California criminal justice agencies will take advantage of the opportunities to do their jobs more efficiently and effectively.

[322] The agreement between A.R.R.E.S.T. and Los Angeles to share data via COPLINK uses the term "Information Ownership," but goes onto describe the responsibilities each party has to maintain the data it inputs into the system. Thus, "ownership" is not referring to intellectual property rights, but to a contractually assigned obligation to maintain one's own data. INTERGOVERNMENTAL AGREEMENT BETWEEN AUTOMATIC RECORDS RETRIEVAL AND ELECTRONIC SHARING TECHNOLOGY (A.R.R.E.S.T.) AND LOS ANGELES COUNTY SHERIFF'S DEPARTMENT, *supra* note 310, at 3.

APPENDIX: CLETS AND OTHER INFORMATION SHARING NETWORKS

> *"Will we have an integrated system in which everyone who routinely works with the criminal justice system (including law enforcement, social services, schools, courts, prosecutors, public defenders, corrections, probation and parole offices) has easy, cheap and quick access to accurate and relevant information? . . . The issues now are not technological. The issues are those of governance, accountability, responsibility and budgets. The issue is one of leadership."*[323]

Criminal justice agencies have long recognized the benefits of integrated criminal justice information systems: more information, accessed quickly, for efficient and effective law enforcement. [324] In 1965 the California State Legislature enacted Government Code section 15152,[325] directing the state Attorney General to establish and maintain a "statewide telecommunications system of communication for the use of law enforcement agencies."[326] This system, known as the California Law Enforcement Telecommunications System (CLETS), has greatly expanded since it became operational in April of 1970.[327] In its first month CLETS processed 558,000 messages, which were mostly requests for information from paper files.[328] Technological advances have made the transfer of vast

---

[323] J. Clark Kelso, *Integrated Criminal Justice Technologies: An Introduction*, 30 MCGEORGE L. REV. 1, 1, 3 (1998)

[324] *See, e.g.*, CALIFORNIA JUDICIAL COUNCIL, REPORT ON THE COMMISSION ON THE FUTURE OF CALIFORNIA COURTS: JUSTICE IN THE BALANCE 101-14 (1994) (Strategic plan with vision of "a comprehensive statewide justice data network" by 2020); Janet Reno, *Justice and Public Safety in the Twenty-First Century*, 30 MCGEORGE L. REV. 5, 7 (1998) ("The criminal justice community needs the capability of linking information rapidly in order to solve crimes, and more importantly, to prevent crimes."); OFFICE OF TECHNOLOGY ASSESSMENT, UNITED STATES CONGRESS, AN ASSESSMENT FOR ALTERNATIVES OF A NATIONAL COMPUTERIZED CRIMINAL HISTORY SYSTEM, at ix (1982), *available at* http://www.scribd.com/doc/4100439/8203 ("To the extent that a national [data] system provides information that is more complete, timely, and verifiable . . . than is presently available, the system would improve the functioning of the criminal justice process.").

[325] CAL. GOV'T CODE § 15152 (2009).

[326] *Id.*

[327] *Hearings Before the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary*, 93d Cong. 355 (1974).

[328] CLETS Strategic Plan, *supra* note 3, at §2.7.

amounts of data possible, and today, with more than 800,000 users accessing 62,000 terminals statewide, CLETS receives over 2 million messages per day.[329] No longer simply accessing paper files, CLETS now serves as the gateway to dozens of computerized databases with state, national, and international criminal information.[330]

As described in the 2008 CLETS Strategic Plan, these databases include:

- **California Criminal Justice Information Systems (CJIS):** The California DOJ maintains several unique data base applications, such as the Automated Criminal History System, Wanted Persons System, Stolen Vehicle System, Automated Boat System, Automated Firearms System, Automated Property System, Restraining Order file, Supervised Released File, the Missing and Unidentified Persons System, Mental Health Firearms Prohibition System, Armed Prohibitive Persons System, and the Megan's Law. These systems provide critical information to CLETS users in the field.

- **Department of Motor Vehicles (DMV):** CLETS also connects to DMV, which provides drivers license, vehicle registration, occupational licensing, parking citation and automated name index information.

- **National Law Enforcement Telecommunications Systems (NLETS):** CLETS is linked by a direct line to the NLETS in Phoenix, Arizona. This NLETS interface provides backbone service into every state for criminal history information, vehicle registration and drivers license information, hazardous material information, aircraft registration and tracking information, snowmobile registration information, ORION ORI information, crime information from INTERPOL and Canada, national insurance crime information, and administrative message traffic.

- **National Crime Information Center**: CLETS is linked by a direct line to the NCIC in Washington D.C., which provides a computerized index of documented criminal justice information concerning crimes and criminals of national interest. NCIC

---

[329] *Id.* § 2.7.2.
[330] *Id.* § 2.7.

databases include, but are not limited to: the Wanted Persons File; the Violent Felon File; the Foreign Fugitive File; the Missing Persons File; the Unidentified Person File; the U.S Secret Service File Interstate Identification Index; the Securities File; the ORI File; the Stolen Vehicle File; License Plate File; the Boat File; the Article File; the Gun File.

- **Oregon Law Enforcement Data System (LEDS)**: CLETS is linked to the Oregon LEDS for drivers license, stolen vehicle and vehicle/boat registration information, and wanted persons information. [331]

[331] CLETS Strategic Plan, *supra* note 3, at §2.7.1.