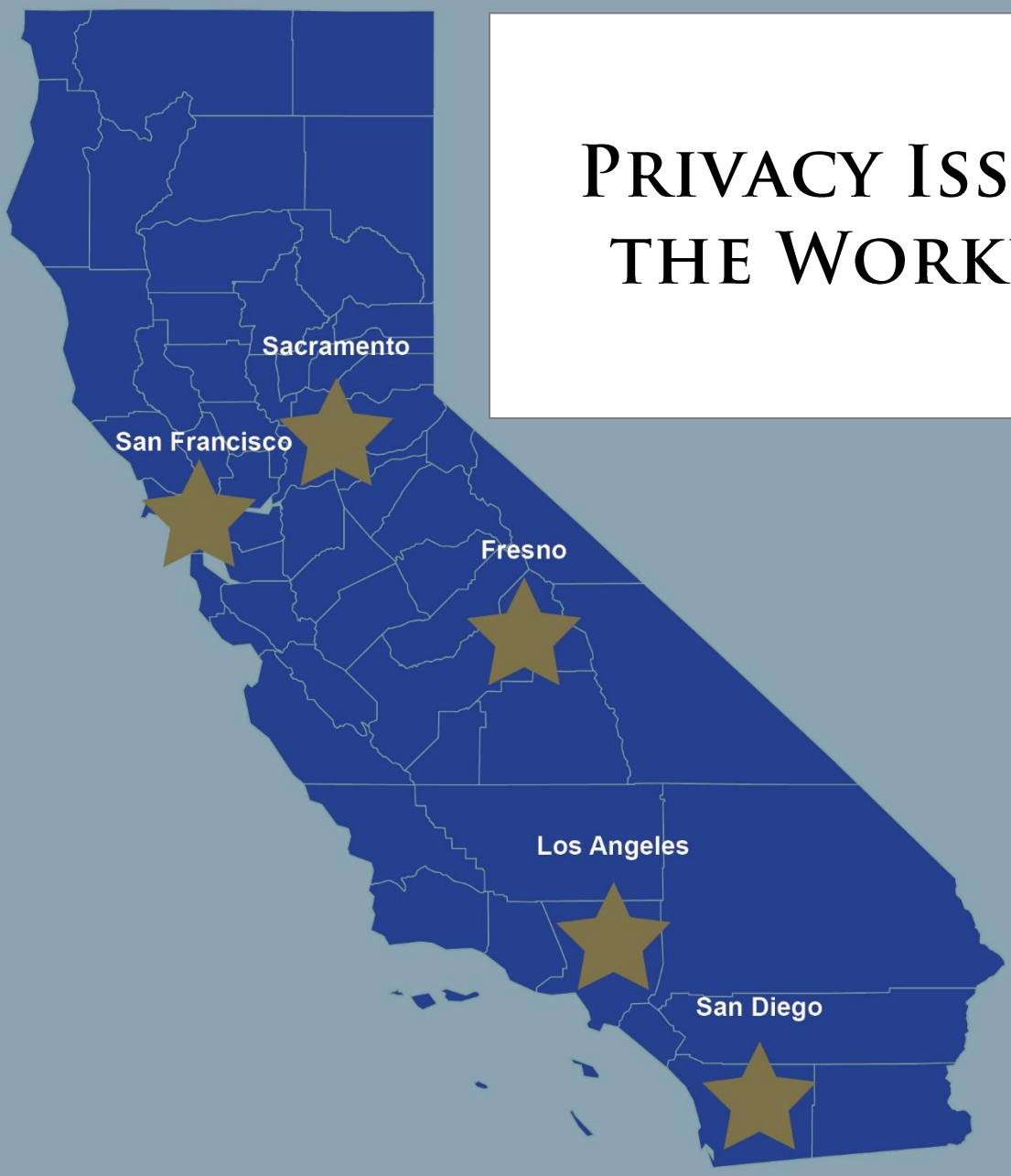
LCW LIEBERT CASSIDY WHITMORE



PRIVACY ISSUES IN THE WORKPLACE

ALL ABOUT THE AUTHORS

With offices in Los Angeles, San Francisco, Fresno, San Diego and Sacramento, the law firm of Liebert Cassidy Whitmore represents Community College District management in all aspects of labor and employment law, labor relations, and education law as well as providing advice and representation in business and facility matters, both transactional and litigation. The Firm's representation of Community College Districts throughout California, encompasses all phases of counseling and representational services in negotiations, arbitrations, fact findings, and administrative proceedings before local, state and federal boards and commissions, including the Public Employment Relations Board, Fair Employment and Housing Commission, Equal Employment Opportunity Commission, Department of Labor and the Office for Civil Rights of the U.S. Department of Education (OCR). In addition, the Firm handles bidding questions, contract review and revision as well as other contracting issues. The Firm regularly handles a wide variety of labor and employment litigation and litigation regarding business and facilities issues, from the inception of complaints through trial and appeal, in state and federal courts.

Liebert Cassidy Whitmore places a unique emphasis on preventive measures to ensure compliance with the law and to avoid costly litigation. For more than thirty years, the Firm has successfully developed and presented training workshops and speeches on all aspects of employment relations for numerous public agencies and state and federal public sector coalitions, including the Community College League of California (CCLC), Association of California Community College Administrators (ACCCA), Association of Chief Human Resources Officers for Community College Districts (ACHRO), California Community College and University Police Chiefs Association (CA CUPCA), Association of Chief Business Officials (ACBO), California Community College Chief Information Service Officers (CCCCISO), Community College Facility Coalition (CCFC), National Employment Law Institute (NELI), and the Public Agency Risk Management Authority (PARMA).

This workbook contains generalized legal information as it existed at the time the workbook was prepared. Changes in the law occur on an on going basis. For these reasons, the legal information cited in this workbook should not be acted upon in any particular situation without professional advice.

TABLE OF CONTENTS 10-21 C

SECTION 7

A. GOAL OF WORKBOOK

Privacy rights implicate many of the actions employers take concerning employees and prospective employees. There is a privacy element to many of the laws that protect applicants and employees in today's workplace. For example, anti-discrimination laws protect applicants and employees not only from discrimination, but also from giving up personal information such as medical condition or national origin that might make them vulnerable to discrimination.

Privacy rights arise from a vast array of federal and state laws that are not only numerous, but often difficult to interpret. Nevertheless, employer obligations and liability in the area of privacy rights rapidly continues to expand. Thus, an understanding of privacy rights is essential to employer due diligence, both to comply with the law and to prevent and defend legal challenges.

This workbook is designed to be a reference tool for employers. It is divided into the major personnel areas impacted by privacy. When faced with an issue in one of these areas, employers can turn to the applicable section of this workbook for an overview of their legal obligations. Of course, no reference guide is a substitute for expert legal counsel. We recommend that employers seek the advice of employment law counsel for difficult or complex employee privacy right questions.

B. TYPES OF EMPLOYER LIABILITY IN PRIVACY ARENA

This workbook covers the specific laws that apply to each of the major personnel areas impacted by privacy. The following, however, is the big picture concerning employer liability in the area of workplace privacy. Employees pursuing a legal challenge against their employers on the basis of privacy rights can rely upon one or more of the following categories of law.

1. FEDERAL AND STATE CONSTITUTIONS

a. Federal Constitution: First, Fourth, and Fourteenth Amendments

While there is no specific federal right to privacy explicitly stated in the United States Constitution, the due process and equal protection clauses of the Fourteenth Amendment of the United States Constitution have been interpreted to confer a right of privacy in certain personal matters.[1] The United States Supreme Court has also interpreted the First and Fourth Amendments to the United States Constitution to confer individual privacy rights in the area of employee free speech, property, association, and personal space.

Fourteenth Amendment employee privacy rights boil down to one of two categories: (1) the right not to have to disclose or uncover personal information;[2] and (2) the right not to have employers interfere with employee personal lives.[3]

The First Amendment to the United States Constitution limits government employers from abridging employees' freedom of speech, religion and association. One example is when an employer attempts to control an employee's political affiliations.[4]

The Fourth Amendment to the United States Constitution protects personal privacy by prohibiting unreasonable searches and seizures. It also protects matters that an individual seeks to preserve as private and that he or she does not knowingly expose to the public. This includes searches of employees and of employee lockers, desks, and personal belongings.

b. California Constitution: Invasion of Privacy Action

Article I, Section 1, of the California Constitution expressly confers a right to privacy. It provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[5] In the leading case interpreting the right to privacy under Article I, Section 1, of the California Constitution, *Hill v. NCAA*,[6] the California Supreme Court identified the core values furthered by the constitutional right as informational privacy and autonomy privacy.

- *Informational privacy* embodies the right against the unauthorized dissemination or misuse of sensitive and confidential information.
- *Autonomy privacy* refers to the federal constitutional tradition of safeguarding certain intimate and personal decisions from government interference.

To prove an invasion of privacy under the California Constitution, a person must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) a serious invasion of the privacy interest. Employers may justify an invasion of privacy by asserting legitimate competing or countervailing interests. If the interests asserted by the employer justify the invasion of privacy, the intrusion does not violate the California Constitution.

The California Supreme Court reaffirmed the above test in *Williams v. Superior Court*[7]. The Court found a flexible approach applies to balancing privacy interests. In *Williams*, the Court permitted the discovery of the names and address of other employees by plaintiffs who may have an interest in a class action to recover wages over the assertion of privacy objections raised by the employer. The Court noted that the *Hill* requirement of a reasonable expectation of privacy was not met on the employees' behalf, as employees could reasonably expect "or even hope" that their contact information would be shared with a plaintiff seeking to vindicate their rights. The Court further explained that not every assertion of a privacy interest under the California Constitution must be overcome by a compelling interest. A compelling interest is only required for "an obvious invasion of an interest fundamental to personal autonomy." However, "when lesser interests are at stake," a "more nuanced framework" applies, "with the strength of the countervailing interest sufficient to warrant disclosure of private information varying according to the strength of the privacy interest itself, the seriousness of the invasion, and the availability of alternatives and protective measures." [8]

The constitutional right of privacy represents a potential limitation on any type of practice or procedure whereby an employer attempts to gather or disseminate private information about an employee or applicant. The actual scope of the limitations placed on the employer must be determined by a careful analysis of the interests involved in each particular case, and by a balancing of those interests.

2. COMMON LAW TORTS

Employees may seek recovery for interference with their privacy rights under several common-law tort theories. The tort of invasion of privacy encompasses four different types of actions.

These are:

- intrusion upon physical solitude or seclusion;
- public disclosure of private facts;
- placing someone in a false light in the public eye;[9] and
- appropriation of name or likeness.

The Government Claims Act establishes the limits of common law liability for a public entity. A public entity is not liable for an injury, whether such injury arises out of an act or omission of the public entity or a public employee or any other person.[10] The common law tort of invasion of privacy may be claimed only against a person in his or her individual (not official) capacity. Case law abolishes common law tort liability for public entities.[11]

Claims for the public disclosure of private facts and for false light have been treated similarly by the courts. To support a claim for one of these privacy violations, an individual must show that there was a public disclosure of private facts concerning him or her. The disclosure must have been an unwarranted disclosure of the individual's private life outside of the realm of legitimate public interest that would be offensive and objectionable to a reasonable person of ordinary sensibilities.[12] Publication disclosure means disclosure to the public generally or to a large group of people.[13]

Publication can be either orally or in writing. In the 2013 case *Ignat v. Yum! Brands, Inc.*[14] , a California court of appeals held an employer was liable for orally disclosing private facts about an employee. In that case, the employee suffered from bipolar disorder and occasionally missed work due to the side effects of her medication. After returning from an absence, the employee's immediate supervisor informed her that she had told everyone in the department that the employee was bipolar. The employee alleged that after her supervisor revealed her condition, her co-workers shunned her and one of them asked her if she was likely to "go postal" at work. When the employee was terminated a few months later, she sued, alleging one cause of action for invasion of privacy for public disclosure of private facts. The trial court granted the employer's motion for summary judgment on the ground that the supervisor did not disclose the employee's condition in writing. The employee appealed, and the Court of Appeal reversed. The Court of Appeals determined that private facts did not have to be disclosed in writing in order to maintain

a cause of action for public disclosure of private facts as facts can be just as widely disclosed through oral media as through written media.

Indirect public disclosure can also support a claim for violation of privacy rights. In the unpublished Ninth Circuit case *Tecza v. University of San Francisco*[15], the university promised in its Student Handbook to keep all information about a student's disability confidential. However, school official discussions in front of others revealed that the student was receiving testing accommodations. This in essence revealed that the student had a disability. Thus, the court permitted a lawsuit to move forward on the theory of breach of contract and tortious disclosure of private facts. The Ninth Circuit also suggested that the lower court should also have considered a claim for violation of the student's constitutional right of privacy.

Colleges should be very careful to treat all medical information confidentially. Supervisors and managers should only be informed of restrictions on the work or duties of employees with disabilities and necessary reasonable accommodations. Co-workers should not be informed of the nature of the disability affecting an employee. Divulging medical information can violate a number of California and federal laws, including the Fair Employment and Housing Act, the California Family Rights Act, the Confidentiality of Medical Information Act (CMIA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

A publication is protected by the "common interest privilege" and is not actionable if it is made by someone with an interest in the matter to another person also holding an interest in the matter.[16] In order for this privilege to apply, the communicator and the recipient must have a common interest, the communication must be made without malice, and the statements must be reasonably calculated to further that common interest.[17] Courts have found an interest exists between an employer and its employees, and between a prior employer and a prospective employer.[18] The privilege to speak can be lost, however, if malice exists in the communication or if the publication goes beyond what is necessary to satisfy the mutual interest that creates the privilege.

Civil Code section 47(c) defines privileged publications and broadcasts that can be used as a defense to claims of defamation, including the common interest privilege. Categories of privileged communications not subject to defamation claims include the following: (1) complaints of sexual harassment made by an employee, without malice, to an employer based on credible evidence; (2) communications between the employer and interested persons, without malice, regarding a complaint of sexual harassment; and (3) communications from an employer, without malice, regarding a current or former employee to a prospective employer of that employee to note if they would rehire the current or former employee and whether such decision is based upon the employer's determination that the employee engaged in sexual harassment. The reference to "without malice" is generally interpreted to mean that the information disclosed must be objective and factual, and not based solely on an opinion.

In contrast, a claim of intrusion upon seclusion does not involve a publication, but rather an unreasonable and highly offensive intrusion upon a person's solitude or private life.[19] These types of claims can arise when an employer requires an individual to divulge information about himself or herself or when an employer conducts an investigation of an employee. To determine whether an intrusion is reasonable, the courts examine factors including whether the means used are abnormal and whether the purpose for intruding is proper.

Not all intrusions are improper. For example, no right of privacy exists for matters or things within the public domain or in places one typically expects others to be.[20]

The final type of privacy tort is seldom, if ever, asserted in the employment relationship. It involves use of someone's name or likeness for commercial purposes without his or her consent.

3. FEDERAL AND CALIFORNIA STATUTES

There is also a vast array of statutes resulting from legislation passed by Congress and the California legislature that prohibit specific types of privacy intrusions and provide bases for recovery by employees, and, in some cases, government prosecutors. For example, Labor Code section 432.7 prohibits an employer from seeking or using arrest records of job applicants. Many of these statutes are discussed in more detail in the sections to which they apply below.

4. CALIFORNIA PUBLIC SAFETY OFFICER'S PROCEDURAL BILL OF RIGHTS ACT

The Public Safety Officers' Procedural Bill of Rights Act (POBR), Government Code section 3300, *et seq*., specifies elements of procedural rights that must be accorded to public safety officers when they are subject to investigation or discipline. Employees subject to this Act include city police officers, county deputy sheriffs, state police and highway patrol officers, D.A. investigators, parole and probation officers, school district security officers, etc. While this Act falls under the category of California Statutes, it bears specific mentioning here because it governs many of the areas of right of privacy of public safety officers in their personnel relationship with employers. The Act is discussed throughout this workbook. While this workbook does not discuss these issues in depth, districts with police departments (as opposed to security officers) must be aware of these rights.

SECTION 2 HIRING INQUIRIES AND BACKGROUND CHECKS

An applicant or employee's right to privacy is weighed against an employer's interest in disclosure.[21] Employers should review their hiring (including promotional) and background check processes to make sure they do not violate applicants' privacy rights. More specifically, employers should verify that inquiries are not made which cannot be justified by some legitimate reason. Hiring and background inquiries should be tailored to determine only if the applicant can perform the essential duties of the job and will otherwise be a quality employee.

Legal Snapshot: Hiring Inquiries & Background Checks	
Applicable laws:	• Constitutional Right of Privacy (Cal. Const. art. I, § 1) • Fair Employment and Housing Act (FEHA), Cal. Gov. Code §§ 12900, *et. seq.* • American with Disabilities Act (ADA), 42 USC §§ 12101, *et. seq.* • Public Safety Officers' Procedural Bill of Rights Act, Cal. Gov. Code §§ 3300, *et seq.* • Various other federal and California statutes • Common law torts
Who and what is protected?:	• Applicants and employees • Personal information that is not job-related
Generally, employers must NOT:	• Ask applicants or employees for personal information that is not job-related • Investigate or seek personal information about applicants or employees that is not job-related
Applicable balancing test:	• Applicants' and employees' interest in keeping personal information private versus employer's legitimate interest in determining qualifications to perform the job in question

A. HIRING INTERVIEWS, QUESTIONNAIRES AND TESTS

All hiring questions must relate to the applicant's ability to perform the job. Questions about religious beliefs, sexual orientation or gender identity, sexual preferences or habits, financial condition, family relationships, and other such private information may not only violate anti-discrimination laws, but may also violate constitutionally protected privacy rights.

The best way to ensure that screening questions are job-related is to evaluate the job position in question. Once the agency is fully aware of the duties and requirements of a job, the agency is in a better position to tailor its interview questions to those that test an applicant's ability to perform that job.

Fraternal Order of Police v. City of Philadelphia[22]
A federal court was called upon to decide the constitutionality of an employment questionnaire that contained questions about medical, psychological, and financial condition, and similar types of information. The questionnaire was given as a condition to reassignment to an elite police unit, and contained the following questions, (that the trial court found violated the employees' right to privacy): "List any physical defects or disability, also list any extended time spent in the hospital for any reason." "Are you now or have you ever been…treated or observed by any doctor or psychiatrist…for any mental or psychiatric condition?" "Do you gamble? a) How often? b) How much?" "List each loan or debt over $1000…." **These questions were ultimately approved by the appellate court but based only on the grounds that the employer issued the questionnaire for a position in an "elite investigations" police unit. The court also held that the individuals applying for the elite unit had a decreased expectation of privacy.**[23]

National Aeronautics and Space Admin. v. Nelson et al [24]**.**
The U.S. Supreme Court held that form questionnaires asking employees about treatment or counseling for recent illegal drug use and asking open-ended questions of the employees' landlords and designated references did not violation the employees' right to information privacy.

The applicants sought contract positions not involving classified material with the Jet Propulsion Laboratory. They were required to complete a Form 85, which asked for: (1) background information, including educational, employment, residential, and military histories; (2) the names of three references; and (3) disclosure of any illegal drug use within the past year, along with any treatment or counseling received for such use. Each of the applicants' references, employers, and landlords were sent a different questionnaire, known as a Form 42, which sought information about the applicant's honesty, trustworthiness, and any adverse information about the applicant.

The U.S. Supreme Court held that, assuming a constitutional right to information privacy exists, the information requested in the forms was "reasonable in light of the Government interests at stake."[25] Under the federal Privacy Act[26], the information collected through the questionnaires is "shielded by statute from 'unwarranted disclosur[e].'"[27] The Privacy Act, which "covers all information collected during the background-check process," permits the Government to "maintain records" about a person "only to the extent the records are 'relevant and necessary to accomplish' a purpose authorized by law."[28] Further, the Act requires "written consent" before the Government can disclosure records relating to a person.[29] These provisions require the Government to take appropriate safeguards to protect the information collected through the questionnaires. Thus, the Government's collection of the information does not violate a constitutional right to information privacy.

DFEH Guidance on Transgender Rights in the Workplace[30]
Employers "should not ask questions designed to detect a person's gender identify, including asking about their marital status, spouse's name, or relation to household members of another."[31] Employers should also "not ask questions about a person's body or whether they plan to have surgery."[32]

B. CONDUCTING REFERENCE AND BACKGROUND CHECKS

Employers have a strong interest in, and may even be statutorily required, to conduct reference or background checks to determine whether job candidates are qualified for employment and whether current employees are qualified for promotion or new assignments. An employer should review its background check process to make sure that it does not violate applicants' privacy rights. Specifically, employers should verify that all inquiries may be justified by a legitimate reason. Background inquiries should be tailored to determine if the applicant can perform the essential duties of the job and will otherwise be a quality employee. These might include questions about the applicant's job skills, disciplinary history, initiative, willingness to learn new tasks, ability to function with co-workers and supervisors, leadership skills, as well as innumerable other job-related factors. By contrast, questions about religious beliefs, sexual preferences or habits, financial condition, family relationships, and other such private information are seldom job-related. The only proper scope of a background check is one that is job related – to ascertain an applicant's qualifications for employment.

1. INFORMATION AVAILABLE FROM PUBLIC SOURCES

In conducting background checks on applicants, many employers resort to publicly available information, including online resources. "Googling" the name of an applicant to search for entries in blogs, or social networking websites like LinkedIn or Facebook has now become a common practice for many employers. This type of online background check does not generally put the prospective employer at legal risk for an invasion of privacy claim because the information obtained online is publicly available, and in many instances it is posted by the job

applicant on his or her LinkedIn or Facebook page.[33] However, an employer may want to employ one of the following approaches in its online background checks:

- Provide notice to the job applicant prior to searching. The employer can either access the site before there is a chance for the job applicant to modify it, or access the site after the applicant has had an opportunity to modify the site/page.
- Access without notice to the job applicant, but provide the applicant with an opportunity to respond to questions concerning online information.
- Access the information without notice and provide no opportunity for the applicant to respond; or
- Not access the online information at all.

While information found on public sites on the Internet is readily available to anyone, caution should be used in relying on this information for exactly the same reason. Information found on the Internet may not accurately reflect the qualities or capacities of the applicant in question. In recent years, for example, there have been numerous reports of false information posted either out of spite or merely as a joke. Even if such information is true or accurate, the question still remains whether it is pertinent to the applicant's qualifications for the position in question. In addition, employers must be careful not to consider information found on the Internet that the employer may not legally consider in screening applicants. For example, social networking pages may provide information about an applicant's protected status such as the applicant's age, race, marital status, religion and similar information. This is information that an employer may not consider in making hiring decisions.

Accordingly, when employers consider online sources of information, employers should be careful in ensuring that: (1) the information found is true and reliable (2) the information is pertinent to the applicant's ability to perform the job, and (3) that the information falls into a category that the employer may legally elicit from the applicant during an interview.

Additionally, Labor Code section 980 prohibits an employer from requiring or requesting that an employee or applicant do any of the following: (1) disclose his or her social media username or password; (2) access his or her personal social media in the presence of the employer; or (3) divulge any personal social media.[34] In short, an employer must not request or require employee personal media usernames or passwords, or seek access to an employee's personal social media, as part of the application process or during employment.

Labor Code section 980 does not affect an employer's "existing rights and obligations" to request an employee to divulge personal social media when "reasonably believed" to be relevant to an investigation into employee misconduct. An employer is also not precluded from asking an employee for a username or password to access employer-issued electronic equipment.

2. OBTAIN A WAIVER

A comprehensive waiver is essential to any successful background check. The waiver should inform the applicant of the categories of information that will be sought from former employers and require that the applicant release the prospective employer and former employers from liability pertaining to the background check.

We recommend that the background examiner meet with the applicant to discuss the waiver and the background check process. The examiner should explain the waiver and the nature of the information that the agency will be seeking. This is an opportunity both to make sure that the applicant is fully informed about the terms of the waiver – reducing or eliminating the possibility of a subsequent successful legal challenge to the waiver – and to give the applicant the opportunity to disclose information that former employers might reveal. This enables the applicant to explain what he or she expects former employers to say, and to give the applicant's perspective on those issues in advance.

3. CONFIDENTIALITY OF SOURCES PROVIDING REFERENCES

Former employers providing references or other subjective information about job candidates may expect or request that the information they provide will be kept confidential. If an individual or agency requests confidentiality, and the prospective employer agrees to provide it, the individual giving the reference may have a privacy right in the information and opinions that he or she shares with the prospective employer, and the employer may be obligated to keep the information confidential.[35] One court blocked an employee's effort to obtain information about confidential references provided by third parties.[36]

Employers should adopt a filing policy that, under appropriate circumstances, protects the privacy rights of the third parties who give confidential references. *These documents should be filed somewhere other than in the personnel file.* Placing references in a manila envelope in a personnel file will not guarantee privacy. The better practice is to file confidential references in a different location.

While it is true that if an employer uses a consumer-reporting agency to conduct a background check, there is an obligation to disclose the report, both federal law[37] and state law[38] permit consumer-reporting agencies to keep source information confidential. Although there are no express provisions permitting employers to keep such information confidential, it would appear to make little sense to allow a consumer-reporting agency to keep the information confidential and to prohibit an employer from doing the same. Furthermore, it is well established by the courts that confidential references may be withheld from employees.[39] Thus, we interpret both laws to permit source information to be kept confidential.

Employees do have a right to inspect their personnel files, but their access to information about third parties who have provided references is restricted. For additional legal discussion on this, refer to Section 5 of this workbook entitled "Personnel Records and Files."

Non-employee applicants for peace officer positions have means at their disposal to examine employment-related information that may be possessed by an employer. For example, the case of *Johnson v. Winter*,[40] addresses the issue of a non-employee applicant who sought background information compiled by the Santa Clara County Sheriff's Department. In general, the basis for the applicant's demand for disclosure was the California Public Records Act.[41] However, the court specifically held that:

> *"We agree, therefore, that to the extent the file contains matters obtained with the understanding implicit or explicit that such matters could be kept confidential, the Court was correct in denying disclosure of those matters. However, we cannot agree that as a matter of law, without a factual determination, all matters contained within Appellant's applicant investigation file are privileged."*[42]

If a peace officer or applicant demands to see his/her background investigation, the department should seek legal counsel's input regarding its obligation to turn over the materials.

4. POLICY FOR RESPONDING TO REFERENCE CHECKS

Privacy rights are an issue, not only for employers who are conducting reference checks, but also employers who are responding to reference checks.

All employers need a background information response policy. Many employers have a policy to provide no information to background investigators, while others permit varying levels of cooperation. It is understandable that many employers choose not to provide information for fear of legal defense costs or liability. But, those employers must recognize that there will be occasions, such as requests from police departments, when the law requires them to provide detailed information about former or current employees.

An employer background response policy should include the following elements:

- ❑ Request that reference be received and maintained in confidence, and only provide information after the prospective employer agrees to provide confidentiality.
- ❑ Pick one of three options and use that option for each and every response. (1) Provide a full disclosure revealing all relevant facts about the applicant's background. (2) Verify the former employee's dates of employment, position and other basic information. (3) Give no information at all.
- ❑ Before preparing to give any response, make sure that the agency has received a written waiver signed by the applicant.
- ❑ Have a centralized procedure for responding to requests. For example, requests for written responses might be distributed to the former employees' supervisors, but all of them should be reviewed by the human resources director, personnel officer, or some other high-level manager. The review official should make sure that the reference is supported by documentation, factual, and consistent with other reference responses.

- ❑ Provide information in writing. While some agencies choose to provide verbal responses, written responses are preferable because they create a clear record of the information provided and help prevent impromptu, emotional outbursts from former supervisors.
- ❑ Apply the policy equally to all current and former employees.
- ❑ Maintain a confidential response process. The only individuals who should discuss and review the agency's reference are those who draft it.
- ❑ Maintain copies of the waiver, written questions, and the agency's responses.

Following a comprehensive policy such as this will help the agency avoid accusations of favoritism, prevent supervisors from drafting emotional, inaccurate or unsupportable references, and preserve the agency's legal defenses.

If an employer does intend to submit fingerprints to the State to obtain a criminal background check, it should use the Department of Justice's Live Scan program. This program enables the Department of Justice ("DOJ") to receive electronically scanned fingerprints and perform records checks. However, the DOJ imposes strict confidentiality requirements and warns employers not to release the results of the criminal background checks.

A Ninth Circuit Court of Appeals case held that no invasion of privacy tort claim was stated where an employer deceived a credit bureau as to its purpose for requesting two credit reports about a job applicant who was bankrupt. The employer and credit bureau's methods were not unreasonably intrusive, the information was used to make a hiring decision, and it was not published or disseminated.[43]

The process by which an agency requests and obtains credit information from job applicants must be structured with standards, guidelines, definitions and limitations precisely indicating the job-related reason for requesting the information.

The Ninth Circuit Court of Appeals held that in the absence of such safeguards, "[t]he risk that an infringement of an important constitutionally protected right might be justified on the basis of individual bias and disapproval of the protected conduct is too great. The very purpose of constitutional protection of individual liberties is to prevent such majoritarian or capricious coercion."[44]

5. CREDIT CHECKS AND "CONSUMER" REPORTS – USE IS LIMITED TO DECISION INVOLVING SPECIFIC JOB CATEGORIES

Labor Code section 1024.5, limits employers, other than certain financial institutions, in using consumer credit reports in connection with employment decisions unless the job in question falls under one of the following categories:

- a managerial position (defined here as an employee who qualifies for the executive exemption from overtime pay under Industrial Welfare Commission Order 4)

- a position in the State Department of Justice
- a sworn peace officer or law enforcement position
- a position for which the employer is legally required to consider credit history
- a position that affords regular access (besides routine processing and solicitation of credit card information in retail establishments) to all the following information of others: bank or credit card account information, Social Security number, date of birth
- a position in which the person is a named signatory on the bank or credit card information of the employer, is authorized to transfer funds on behalf of the employer, or is authorized to enter financial contracts on behalf of the employer
- a position that affords access to proprietary or confidential information
- a position that involves regular access to cash totaling more than $10,000 of the employer, a customer or client during the workday.

Civil Code section 1785.20.5 requires an employer who requests a credit report from an applicant or employee to notify that individual which of the specific exceptions applies to him or her. Additionally, districts should continue to comply with restrictions imposed by the Fair Credit Reporting Act's[45] and the Investigative Consumer Credit Reporting Agencies Act's[46] upon the acquisition and use of credit history information about applicants and employees:

- The scope of any credit history inquiries should be job related.47
- Written notice to the applicant must be provided, giving the applicant the opportunity to receive a copy of the report at no charge.
- If the employer makes an adverse employment decision based in whole or in part upon the report, it must advise the applicant of that fact and provide the name and address of the agency that furnished the report.

Employer Tips: Employers should determine which positions in their agency still allow use of credit reports in connection with employment decisions. They should also re-visit the notice forms they currently use to comply with notice and disclosure provisions and update them to include the new notice requirements.

Districts should keep in mind that Fair Credit Reporting Act and the Investigative Consumer Reporting Agencies Act also impact many other aspects of the background investigation process as discussed below.

a. The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA)[48] is federal legislation that not only restricts the use of credit reports, but also impacts an employer's conduct of reference checks if the employer utilizes the services of a third party to conduct the reference checks. *If an employer conducts reference checks itself, and does not employ the services of a consumer-reporting agency, the employer is not subject to the FCRA.*

The FCRA governs the requisition, distribution, and use of "consumer reports," which, by definition, must be prepared by a "consumer reporting agency":

- A "consumer report" is statutorily defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" which is used or expected to be used for, among other purposes, "employment purposes."[49]
- The FCRA defines "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility on interstate commerce for the purpose of preparing or furnishing consumer reports."[50]

A reference check that is performed by an employer, and is not performed by a consumer-reporting agency, does not fall within the definition of a consumer report and is not governed by the FCRA. Public employers are generally not consumer reporting agencies. On the other hand, if an employer hires a third party, such as a private investigator, to conduct its background and/or reference checks, that person or entity likely meets the definition of a consumer reporting agency.[51]

Damages are available for willful and negligent violations of the FCRA.[52] However, employers should note that liability may be avoided in certain cases where reasonable procedures are developed by an employer to assure compliance.[53]

i. Affirmative Obligations on Employer

If an employer is or utilizes a consumer-reporting agency to conduct a reference or background check, it must undertake the following:

- ❑ Within three (3) days of requesting a report, the employer must make a "clear and conspicuous disclosure" to the applicant in a document that consists solely of the disclosure that a consumer report may be obtained for employment purposes.[54]
- ❑ The applicant must provide written authorization to procure the report.[55]

- ❑ The employer must certify in writing to the consumer-reporting agency that the required disclosures have been made to the applicant, that the applicant has provided written authorization to procure the report, that the information in the report will not be used in violation of any applicable Federal or State equal employment opportunity law or regulation.[56]
- ❑ Upon written request by the applicant (made within a reasonable period of time after the receipt by the applicant of the above disclosure), the employer must make a complete and accurate disclosure of the nature and scope of the investigation that the consumer reporting agency has been requested to perform.[57]
- ❑ Prior to taking an adverse action (a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee)[58] based in whole or in part upon the report, the employer shall provide to the applicant a copy of the report, as well as a written description of the rights of the employee as prescribed by the Federal Trade Commission.[59]
- ❑ Upon taking adverse action, an employer must provide oral, written, or electronic notice of: 1) the adverse action to the applicant, 2) the name, address, and telephone number of the consumer reporting agency that furnished the report, 3) the applicant's right to obtain a free copy of the report, 4) the applicant's right to dispute the accuracy or completeness of any of the information in the report. The employer must also notify the applicant that the consumer-reporting agency did not make the decision to take the adverse action and that it is unable to provide the consumer the specific reasons why the adverse action was taken.[60]
- ❑ The employer may not use the report for any purpose other than that for which it was authorized by the applicant to be procured.[61]

> ***Note:*** *There are also significant restrictions placed upon consumer reporting agencies, including the obligation to reinvestigate matters included in a report which are disputed by an applicant.*

ii. Restrictions on Information in Consumer Report

There are strict limitations on the types of information that may be included in a consumer report.[62] The following is a list of the categories of information which must be excluded:

- ❑ Cases under Title 11 or under the Bankruptcy Act that, from the date of entry of the order for relief or the date of adjudication, as the case may be, pre-date or precede the report by more than 10 years.
- ❑ Civil suits, civil judgments, and records of arrest that, from date of entry, pre-date or precede the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period.
- ❑ Paid tax liens which, from date of payment, pre-date or precede the report by more than seven years.

- ❑ Accounts placed for collection or charged to profit and loss which pre-date or precede the report by more than seven years.
- ❑ Any other adverse item of information, other than records of convictions of crimes which pre-dates or precedes the report by more than seven years.

The above limitations do not apply when a report will be used in connection with the employment of any individual at an annual salary which exceeds $75,000.[63]
In any case, a consumer-reporting agency is prohibited from furnishing an employer with a report containing medical information unless the applicant consents.[64] The FCRA does not identify the requirements for such consent, but we recommend that it be in writing, signed by the applicant, and be drafted in conformity with the Confidentiality of Medical Information Act, discussed later in this workbook. Also, employers are cautioned not to seek medical information until after a conditional offer of employment has been made.

b. The Investigative Consumer Reporting Agencies Act

The Investigative Consumer Reporting Agencies Act (ICRA)[65] is California legislation which, in many respects, mirrors the Fair Credit Reporting Act (above.)

> ***Note:*** *Unlike the FCRA, even if an employer conducts reference checks itself, and does not employ the services of a consumer-reporting agency, the employer may still be subject to the Act though the requirements are less onerous when reference checks are conducted in-house.*[66]

The requirements of the Act are triggered when an employer utilizes an "investigative consumer reporting agency" (ICRA) to prepare an "investigative consumer report" regarding a "consumer":

- An ICRA is statutorily defined as "any person who for, monetary fees or dues, engages in whole or in part in the practice of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning consumers for the purposes of furnishing investigative consumer reports to third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes . . ."[67]
- An investigative consumer report is a "report in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through any means . . ."[68] Reference checks commonly address the character, reputation, and mode of living of prospective employees and would appear to meet the definition of an investigative consumer report. However, for the purpose of AB 22's limitation on the job positions for which a credit report may be sought, "consumer credit report" does not include a report that (a) verifies income or employment and (b)

does not include credit-related information, such as credit history, credit score, or credit record.[69]

Any third party who is hired to conduct reference checks on behalf of an employer would appear to meet the definition of an ICRA.

i. Employer Obligations When a Reference Check is Conducted By an ICRA

When a background investigation is conducted by an ICRA instead of being conducted in-house there are numerous restrictions on the conduct of the investigation.

- The Act requires an ICRA to permit a consumer to inspect its files, "except that the sources of information, other than public records and records from data bases available for sale, acquired solely for use in preparing an investigative consumer report and actually used for no other purpose need not be disclosed."[70]
- At any time before the report is procured or caused to be made, the employer must make a "clear and conspicuous disclosure" to the applicant in a document that consists solely of the disclosure that: (i) An investigative consumer report may be obtained, (ii) the permissible purpose of the report is identified, (iii) the disclosure may include information on the consumer's character, general reputation, personal characteristics, and mode of living, (iv) identifies the name, address, and telephone number of the investigative consumer reporting agency conducting the investigation, and (v) notifies the consumer in writing of the nature and scope of the investigation requested, and also including a summary of the right to inspect the report.[71]
- Also, the employer must "provide the consumer a means by which the consumer may indicate on a written form, by means of a box to check, that the consumer wishes to receive a copy of any report that is prepared. If the consumer wishes to receive a copy of the report, the recipient of the report shall send a copy of the report to the consumer within three business days of the date that the report is provided to the recipient, who may contract with any other entity to send a copy to the consumer. The notice to request the report may be contained on either the disclosure form . . . or a separate consent form. The copy of the report shall contain the name, address, and telephone number of the person who issued the report and how to contact that person."[72]
- The applicant must provide written authorization to procure the report, including but not limited to, circumstances when the report will contain medical information.[73]
- The employer must certify to the ICRA that it has made the above disclosures, and must agree to provide a copy of the report to the applicant.[74]
- "Whenever…employment…is denied…under circumstances in which a report regarding the consumer was obtained from an investigative consumer reporting agency, the user of the investigative consumer report shall so advise the consumer against whom the adverse action has been taken and supply the name and address of the investigative consumer reporting agency making the report."[75]

- ❑ After reviewing the report, if the consumer believes that the report is incomplete or inaccurate, the consumer may dispute the completeness or accuracy of "any item of information contained in his or her file."[76]
- ❑ The Act establishes procedures for reinvestigation of the disputed matters and notice to the individual(s) who provided the information that the information is being disputed.[77]

ii. Restrictions on Information in the Report

Similar to the FCRA, the Act imposes strict limitations on the types of information which may be included in a report that is prepared by an ICRA. The following types of information may not be included in a report:

- ❑ Bankruptcies that, from the date of adjudication, pre-date or precede the report by more than 10 years.
- ❑ Suits that, from the date of filing, and satisfied judgments that, from the date of entry, pre-date or precede the report by more than seven years.
- ❑ Unsatisfied judgments that, from the date of entry, pre-date or precede the report by more than seven years.
- ❑ Unlawful detainer actions where the defendant was the prevailing party or where the action was resolved by settlement agreement.
- ❑ Paid tax liens that, from the date of payment, pre-date or precede the report by more than seven years.
- ❑ Accounts placed for collection or charged to profit and loss that pre-date or precede the report by more than seven years.
- ❑ Records of arrest, indictment, information, misdemeanor complaint, or conviction of a crime that, from the date of disposition, release, or parole, pre-date or precede the report by more than seven years. These items of information shall no longer be reported if at any time it is learned that, in the case of a conviction, a full pardon has been granted or, in the case of an arrest, indictment, information, or misdemeanor complaint, a conviction did not result; except that records of arrest, indictment, information, or misdemeanor complaints may be reported pending pronouncement of judgment on the particular subject matter of those records.
- ❑ Any other adverse information that pre-dates or precedes the report by more than seven years.[78]

> ***Note*** *that the above regulations do not apply if the report is to be used by an employer who is explicitly required by a governmental regulatory agency to check for such records. However, this provision is questionable given that no parallel provision exists in the FCRA, and federal law preempts state law.*

In addition, Civil Code section 1786.40, provides that an employer that decides not to hire an applicant based upon a report shall notify the applicant of the decision and the name and address of the reporting agency. The Act also imposes restrictions on the information that may be included in a report which is collected from friends, neighbors, relatives, and acquaintances:

> *An investigative consumer reporting agency shall not prepare or furnish an investigative consumer report on a consumer that contains information that is adverse to the interest of the consumer and that is obtained through a personal interview with a neighbor, friend, or associate of the consumer or with another person with whom the consumer is acquainted, or who has knowledge of the item of information, unless either: (1) the investigative consumer reporting agency has followed reasonable procedures to obtain confirmation of the information from an additional source that has independent and direct knowledge of the information, or (2) the person interviewed is the best possible source of the information.*[79]

iii. Employer Obligations When Reference Check is Conducted in-House

While the most stringent requirements of the ICRA apply to employers who utilize the services of consumer reporting agencies, there are still some disclosure requirements placed upon employers that do not. Specifically, the ICRA provides:

- Unless the applicant has elected not to receive them,[80] an employer must provide a copy of any public record (records documenting an arrest, indictment, conviction, civil judicial action, tax lien, or outstanding judgment) that is obtained for employment purposes within seven (7) days after receipt of the information, whether the information is received in a written or oral form.[81]
- Even if the applicant has elected not to receive any information, if an employer takes any adverse action (a denial of employment or any decision made for an employment purpose that adversely affects any current or prospective employee) as a result of receiving such public records, the employer shall provide to the consumer a copy of the public record.[82]
- The election to receive or not to receive any public records that may be obtained is to be made on a form provided by the employer and described as following: "any person shall provide on any job-application form, or any other written form, a box that, if checked by the consumer, permits the consumer to waive his or her right to receive a copy of any public record obtained pursuant to this selection."[83]

iv. FACT ACT may require employer investigation of furnished consumer data

The Fair and Accurate Credit Transactions Act of 2003 (FACT) amended the FCRA to increase the accuracy and integrity of information furnished to consumer reporting agencies. There are certain situations in which an employer can be a furnisher of data pursuant to FCRA. The FTC determined that certain companies, such as reference check providers, are consumer-reporting agencies under FCRA. Therefore, employers that provide payroll and other employee related information to consumer reporting agencies as part of outsourced services will also be considered furnishers under FCRA.

These regulations require that employers who furnish information to consumer reporting agencies investigate information disputed by the subject employee. The employer is required to conduct a reasonable investigation to determine the validity of the employee's dispute. These contemplated disputes require that the employee provide the employer with sufficient information regarding the employment relationship and the "inaccurate" information to enable the employer to conduct an investigation.

The investigation must be completed within 30 days (an additional 15 days is allowed if an employee provides new information.) If the information furnished by the employer was inaccurate, the employer must correct it by providing notification to each consumer-reporting agency that received the incorrect information.

v. Frivolous or Irrelevant Disputes

Not all disputes must be investigated – identifying information, such as name, date of birth, social security number need not be investigated. Also, if the employee doesn't provide sufficient information to investigate, the employer need not investigate. The employer must notify the employee that the matter will not be investigated because it is frivolous or irrelevant within five (5) days of making that determination. If the employer needs additional information to conduct an investigation, the employer should request it.

Furnished information should be accurate – i.e., factually correct and have integrity, i.e., substantiated by business records. It should be presented in a form and manner to minimize the possibility it may be incorrectly reflected in any report prepared by a consumer-reporting agency. (16 C.F.R. § 660.2(a),(e).)

6. PEACE OFFICER BACKGROUND INVESTIGATIONS

When hiring peace officers, the law mandates that a thorough background investigation be performed. Government Code section 1031 provides:

> *Each class of public officers or employees declared by law to be peace officers shall meet all of the following minimum standards:*
>
> *(c) Be fingerprinted for purposes of search of local, state, and national fingerprint files to disclose any criminal record…*
>
> *(d) Be of good moral character, as determined by a thorough background investigation…*
>
> *(f) Be found to be free from any physical, emotional, or mental condition which might adversely affect the exercise of the powers of a peace officer. Physical condition shall be evaluated by a licensed physician and surgeon. Emotional and mental condition shall be evaluated by a licensed physician and surgeon or by a licensed psychologist who has a doctoral degree in psychology and at least five years of postgraduate experience in the diagnosis and treatment of emotional and mental disorders…*

The California Commission on Peace Officers Standards and Training (P.O.S.T.) has instituted regulations in furtherance of the requirements imposed by Government Code section 1031 which set forth additional procedures and requirements for agencies.

As discussed above, the FCRA and ICRA impact the conduct of background investigations, even for peace officers. One significant concern for employers in this regard are the restrictions on the types of information that may be included in a background report prepared by a third party. While California can provide an exception to these restrictions when an employer is required by a regulatory agency, e.g., P.O.S.T., to consider such information, federal law provides no such exception. If the restrictions on the information which may be reported by a third party do not permit an agency to conduct an adequate background investigation, the agency should give serious consideration to conducting the investigation in-house in which case the restrictions do not apply.

C. CRIMINAL RECORDS

California law restricts access to and use of information about job applicants' criminal histories. Labor Code section 432.7 describes permissible and impermissible uses for criminal information. The rules in this section raise two distinct classes of criminal records; those that an employer may not use and those that it may use.

1. EXEMPTION FROM STATUTE LIMITING BACKGROUND CHECKS THAT REVEAL CONVICTION HISTORY

Government Code section 12952 makes it an unlawful employment practice for an employer with five or more employees to do any of the following:

- To include on any application for employment, before the employer makes a conditional offer of employment, any question that seeks the disclosure of the applicant's conviction history.
- To inquire into or consider the conviction history of the applicant, including any inquiry about conviction history on any employment application, until after the employer has made a conditional offer of employment to the applicant.
- To consider, distribute, or disseminate information about any of the following while conducting a conviction history background check in connection with any application for employment:
  - An arrest not followed by a conviction, except when permitted under Labor Code section 432.7(a)(1) and Labor Code section 432.7(f)
  - Referral to or participation in a pretrial or posttrial diversion program
  - Convictions that have been sealed, dismissed, expunged, or statutorily eradicated pursuant to the law.
- To interfere with, restrain, or deny the exercise of, or the attempt to exercise, any right provided by this section.[84]

Government Code section 12952 does not prevent an employer from conducting a conviction history background check not in conflict with the above restrictions on criminal background checks.[85] In addition, the above restrictions on criminal background checks do not apply to the following circumstances:

- To a position for which a state or local agency is otherwise required by law to conduct a conviction history background check.
- To a position with a criminal justice agency, as defined in Penal Code section 13101.
- To a position as a Farm Labor Contractor as described in Labor Code section 1685.
- To a position where an employer or its agent is required by any state, federal, or local law to conduct a criminal background checks for employment purposes or to restrict employment based on criminal history.[86]

If an employer intends to deny an applicant a position of employment solely in or in part because of the applicant's conviction history, the employer must "make an individualized assessment of whether the applicant's conviction history has a direct and adverse relationship with the specific duties of the job that justify denying the applicant the position."[87] In making this assessment, the employer must consider:

- The nature and gravity of the offense or conduct,
- The time that has passed since the offense or conduct and the completion of the sentence, and
- The nature of the job held or sought.[88]

The employer may, but is not required to, put the results of this individualized assessment in writing.[89]

If the employer makes a preliminary decision that the applicant's conviction history disqualifies the applicant from employment, the employer must notify the applicant of the preliminary decision in writing.[90] The notification may, but is not required to, justify or explain the employer's reasoning for making the preliminary decision.[91] The notice must contain all of the following:

- Notice of the disqualifying conviction or convictions that are the basis for the preliminary decision to rescind the offer
- A copy of the conviction history report, if any
- An explanation of the applicant's right to respond to the notice of the employer's preliminary decision before that decision because final and the deadline by which to respond. The explanation must inform the applicant that his/her response may include submission of evidence challenging the accuracy of the conviction history report that is the basis for rescinding the offer, evidence of rehabilitation or mitigation circumstances, or both.[92]

The applicant must have at least five business days to respond to the notice before the employer makes the final decision. If, within the five business days, the applicant notifies the employer in writing that he/she disputes the accuracy of the conviction history report that was the basis of the preliminary decision to rescind the offer and is taking specific steps to obtain evidence in support, the applicant has five additional business days to respond to the notice.[93]

The employer must consider the information submitted by the applicant before making a final decision.[94] If the employer makes a final decision to deny an application solely or in part because of the applicant's conviction history, the employer must notify the applicant in writing of all of the following:

- The final denial or disqualification. The employer may, but is not required, to justify or explain the employer's reasoning for making the final denial or disqualification.
- Any existing procedure that the employer has for the applicant to challenge the decision or request for reconsideration.
- The right of the applicant to file a complaint with the department.[95]

While the statute does not expressly address this issue, Government Code section 12952 does not apply to community college district and K-12 school districts. Both community college districts and K-12 districts are required to fingerprint all employees and thus, we can reasonably conclude that they are required by law to conduct a conviction history background check on employees. Thus, they would be excluded from the restrictions on considering conviction history under Government Code section 12952(d)(4), which excludes employers required by any state, federal, or local law to conduct criminal background checks for employment purposes or to restrict employment based on criminal history.[96]

2 CRIMINAL RECORDS AN EMPLOYER MUST NOT SEEK OR USE

Under Labor Code section 432.7 employers may not ask applicants or current employees to provide, and cannot refuse to hire or promote them, on the basis of any of the following information:

- An arrest or detention that did not result in conviction. A conviction is a guilty or nolo contendere (no contest) plea, criminal conviction, or other finding of guilt. A conviction does not require a criminal sentence or other punishment.
- Marijuana convictions more than two years old[97].
- Referral to and participation in any pretrial or post-trial diversion program. There are numerous forms of diversion programs provided under the Penal Code, Vehicle Code and elsewhere.

This section also prohibits law enforcement agencies from providing either of the above types of information to prospective employers.

Applications for employee should clearly and ambiguously direct applicants not to disclose information regarding arrests that did not result in conviction and marijuana convictions more than two years old.[98] California Labor Code sections 432.7 and 432.8 prohibit employers from requiring that records of arrests that did not result in conviction and marijuana convictions more than two years old be listed on the initial application form. This prohibition does not apply to persons applying for jobs as peace officers, with criminal justice agencies, and with certain health facilities as defined in Health and Safety Code section 1250.[99]

While it might be tempting to use your agency's police department as a resource to learn this information, it is imperative that you refrain from doing so. Both the police department employees who provide the information and any individuals in the agency who use the information against job applicants could face civil and criminal sanctions. An intentional violation of section 432.7 is a misdemeanor. Unsuccessful job applicants or current employees denied promotions, assignments or other benefits based on such information may sue for damages and attorney's fees. They may also obtain treble damages if they prove that the employer intentionally obtained or used the prohibited information.

In addition, the timing of when an agency asks for criminal conviction information matters. Labor Code section 432.9 (effective July 1, 2014) prohibits a state or local agency from asking an applicant to disclose information regarding the conviction history of the applicant, until the agency has determined that the applicant meets the minimum employment qualifications for the position as stated in any notice issued for the position.[100] This prohibition applies to both oral and written inquiries and specifically applies to inquiries about conviction history on an employment application.[101] However, Labor Code section 432.9 does not prevent a state or local agency from conduct a conviction history background check after determining that the applicant meets the minimum employment qualifications as stated in the notice for the position.[102] There are also some exceptions to the Labor Code section 432.9 restriction on when an agency can inquire about an applicant's criminal conviction history. [103] The restriction does not apply to:

- Positions for which a state or local agency is otherwise required by law to conduct a conviction history background check;
- Positions within a criminal justice agency; or
- Individuals working on a temporary or permanent basis for a criminal justice agency on a contract basis or on loan from another governmental agency.[104]

3. CRIMINAL RECORDS AN EMPLOYER MUST OBTAIN

a. Law Enforcement

Police departments, the Department of Justice and any other agency employing peace officers may obtain and use arrest information when deciding whether to hire peace officer candidates. Section 432.7 recognizes that peace officers are held to a higher standard than other classes of employees. However, these agencies may not automatically dismiss applicants because they have an arrest record. The arrest might have been an isolated incident, clearly in error or not cause for concern for any of a number of reasons. Law enforcement agencies should conduct their own investigation into the arrest. At a minimum the agency should discuss the arrest information with the applicant to attempt to determine the facts before making any decision.

b. Public Health Facilities

Agencies operating public health facilities may ask job applicants questions about certain types of arrests. They may ask applicants who would work with patients if they have ever been arrested for a violation of Penal Code section 290. The purpose of this exception is to learn if an applicant might harm patients.

c. Minors

Public Resources Code section 5164 mandates that any city, county, or special district that hires a person for employment, or hires a volunteer to perform services, at a *park, playground, recreational center or beach*, in a position having supervisory or disciplinary authority over any minor shall complete an application that inquires as to whether or not that individual has been convicted of specified criminal offenses.

Likewise, Penal Code section 11105.3 provides that an employer may request from the Department of Justice records of convictions and/or arrests pending adjudication for specified offenses (including sex offenses against minors, theft, robbery, burglary, or any felony) with regard to an applicant for a position in which the applicant would have supervisory or disciplinary power over a minor or any person under his or her care.

d. Sex Crimes and Controlled Substance Offenses - Schools

Education Code sections 87405 and 88022 prohibit districts from employing or retaining individuals convicted of sex crimes or controlled substance offenses. Education Code section 87010 defines "sex crimes" and Education Code section 87011 defines "controlled substance offense." If, however, a court reverses an individual's conviction and acquits the individual of the offense in a new trial; or a district attorney dismisses the charges against the individual, a district may employ the individual.

In addition, a district *may not deny or refuse to retain an individual solely on the basis* that the individual was convicted of a sex or controlled substance offense if: (1) the individual obtained or applied for a certificate of rehabilitation and pardon; (2) the individual completed probation; and (3) the information or accusation has been dismissed.

A district, however, *may* employ or retain an individual convicted of a sex or controlled substance offense if: (1) the governing board of the district determines that the individual has been rehabilitated for at least five years; (2) the individual received a certificate of rehabilitation and pardon; or (3) the accusation or information against the individual was dismissed and the individual has been released from all disabilities and penalties resulting from the offense. Moreover, Education Code sections 87405 and 88022 permit a district to employ an individual convicted of a controlled substance offense if the district's governing board determines that the individual has been rehabilitated for at least five years.

Aside from sex and controlled substance convictions, a district should not automatically disqualify applicants with criminal records. Rejecting all applicants with criminal records might disproportionately impact individuals within a protected class and lead to a disparate impact race discrimination lawsuit against a district. Districts should consider an applicant's individual circumstances in determining whether the conviction is sufficiently serious, recent, and job related enough to disqualify the applicant from the job.

4. CRIMINAL RECORDS AN EMPLOYER MAY OBTAIN

The California Penal Code permits public agencies to obtain criminal history information from the Department of Justice. Penal Code section 11105 requires the Department of Justice to maintain the following information about individuals with criminal records:

- Name,
- Date of birth,
- Physical description,
- Fingerprints,
- Photographs,
- Dates of arrest and arresting agencies,
- Booking numbers,
- Charges, and
- Dispositions.

This section permits the Department of Justice to release (subject to the restrictions of Labor Code section 432.7, Penal Code section 11105.3, and Public Resources Code section 5164) this information to any local public agency if the agency's governing body authorizes its management staff to obtain criminal background data in the employment application process. Prospective employers should specifically request that the Department of Justice only provide information about convictions, or arrests pending adjudication.

Once the employer obtains an applicant's criminal record, it must determine whether it will hire the individual or withdraw a conditional offer of employment. An employer should not automatically disqualify applicants with criminal records. Rejecting all applicants with criminal records might disproportionately impact individuals within a protected class and lead to a disparate impact race discrimination lawsuit against the agency. The agency should therefore consider all of the circumstances related to the conviction and whether it has any relationship to the job. The following factors should be given consideration:

- Nature and seriousness of the offense
- Circumstances related to the conviction

- Repeat offenses
- Relationship between the job and the conviction
- Length of time since last conviction
- Age at the time of conviction
- Evidence of rehabilitation

Deciding whether to hire an individual with a criminal record requires thorough analysis and assessment. Human resources professionals know that they must assess each candidate's ability to perform the essential functions of a job. The employer needs to consider the applicant's individual circumstances to determine if the conviction is sufficiently serious, recent and job-related to disqualify him or her from the job.

In 2012, the Equal Employment Opportunity Commission (EEOC) issued enforcement guidance regarding the consideration of arrest and conviction records in employment decisions.[105] The enforcement guidance reaffirms two uses of criminal history information by employers that may violate Title VII: (1) "disparate treatment", when the employer treats applicants with the same criminal history differently because of their race, color, religion, sex, or national origin; and (2) "disparate impact", where even though the employer applies criminal record exclusions uniformly, the exclusions operate to "disproportionately and unjustifiably" exclude people of a particular race or national origin. The employer can overcome a showing of disparate impact by demonstrating that the exclusion is "job related and consistent with business necessity".[106]

The EEOC Enforcement Guidance sets forth two circumstances where an employer may consistently meet the "job related and consistent with business necessity" defense.[107] These are:

- The employer "validates the criminal conduct exclusion for the position in question in light of the Uniform Guidelines on Employee Selection Procedures (if there is data or analysis about criminal conduct as related to subsequent work performance or behaviors)"; or
- The employer "develops a targeted screen considering at least the nature of the crime, the time elapsed, and the nature of the job. . . . The employer's policy then provides an opportunity for an individualized assessment for those people identified by the screen, to determine if the policy as applied is job related and consistent with business necessity."

The EEOC Enforcement Guidance further advises that: "while Title VII does not require an individualized assessment in all circumstances, the use of a screen that does not include an individualized assessment is more likely to violate Title VII."108 Thus, we recommend performing an individualized assessment for applicants to determine if the policy as applied is job related and consistent with business necessity.

D. FINGERPRINT RECORDS

Education Code section 88024 mandates that a district must fingerprint each employee in a nonacademic position within 10 working days of the employee's first day of work. The employee must have a local law enforcement agency with jurisdiction over the district fingerprint her or him. Education Code section 88024 further specifies that the law enforcement agency must use an 8 x 8 fingerprint card and include a personal description of the employee or applicant. The law enforcement agency must then transmit the cards to the Department of Justice.

Education Code section 87013 similarly requires that a district fingerprint each employee in an academic position within 10 working days of the employee's first day of employment. The employee must have a local law enforcement agency with jurisdiction over the district fingerprint her or him. The law enforcement agency must then transmit the fingerprints to the Department of Justice. If, however, the employee previously worked at a California school or community college, the employee does not need to comply with this section.

E. POLYGRAPH EXAMINATIONS

1. EMPLOYEES IN GENERAL

Labor Code section 432.2, prohibiting the use of polygraph examinations, only applies to private employers. But, Government Code section 3307 protects public safety officers from compelled polygraph examinations during the course of employment.

While there is no existing state statutory prohibition which applies to public sector employees in general, the California Supreme Court held in *Long Beach City Employee Assn. v. City of Long Beach*,[109] that non-safety public employees could not be required to submit to polygraph examinations.

The Court in the Long Beach City Employee Assn. case stated that the mind is a "quintessential zone of human privacy" which a polygraph examination is specifically designed to overcome by 'compelling communications of thoughts, sentiment, and emotions' which the examinee may have chosen not to communicate." The Court further expressed concern that repressed beliefs, guilt feelings and fantasized events, not just actual events, can impact the polygraph examination results. The court noted that pre-employment polygraph testing, which has frequently been used as a fishing expedition, is inherently unreliable, and often involves "shockingly intrusive questions." The Court did not reach the issue of whether applicants for public sector employment could be required to take a polygraph test. Part of the rationale of the *Long Beach* decision, however, was that there was no reason to treat public sector employees differently with respect to polygraph examinations than private sector employees, who are protected by statute from such examinations. Thus, polygraph exams for non-sworn position applicants are not recommended. The examinations should only be given where the agency can show a compelling reason for requiring the test. Additionally, if polygraph examinations are given to applicants (as they typically are to peace officer applicants), the questions must be narrowly tailored to serve the legitimate interests of the agency.

In *Thorne v. City of El Segundo*,[110] the defendant city had no standards limiting the scope and areas for questioning during a police applicant polygraph examination. As a result, the examiner intruded into off-duty non-job-related sexual activities. The court deemed that line of questioning so invasive that it could not be justified under any level of scrutiny. To avoid this situation, employers should thus provide the examiner with a standard list of questions and instruct the examiner not to deviate from the identified line of questioning. In any polygraph examination, employers should only ask questions related to the job duties of the specific position.

The court in the *Long Beach* case, for example, found that the following questions impermissibly violated the examinee's privacy rights: 1) Have you had any major operations within the past ten years?; 2) Have you had sex with men or animals?; 3) How often do you masturbate?; 4) Do you cheat on your wife?; 5) Have you ever had an automobile accident while you were driving?; 6) Have you written any bad checks in the past three years?; 7) Have you suffered a nervous breakdown within the past ten years? These questions were found to be entirely unrelated to the person's employment duties, and thus beyond the permissible scope of questioning.

2. PUBLIC SAFETY OFFICERS

Under Government Code section 3307, the POBR gives a peace officer the absolute right to decline to take a polygraph examination even when the police officer is under investigation for suspected criminal activity.[111] Admissions made as a result of a threatened polygraph examination will be excluded by a court in considering the merits of resulting disciplinary action.[112] Even if a police officer were to submit to a voluntary polygraph examination, the results are probably not admissible in a subsequent administrative hearing.[113]

However, police departments may require polygraph examinations for officers who voluntarily seek to be promoted or transferred into specialized divisions where work is unusually sensitive and requires the highest level of integrity; this requirement has been held to not invade police officers' right to privacy.[114]

F. RESPONDING TO REFERENCE CHECKS

While conducting a thorough background investigation is an important human resources function, it is equally important to provide information about current or former employees without creating legal liability for the agency. This section discusses employers' obligations to provide information, potential legal pitfalls associated with doing so, and legal protections which are available.

1. TORT CLAIMS

There are numerous civil "tort" claims an employee may raise related to the provision of a job reference. A tort cause of action is a claim that one individual has wrongfully harmed another. The following are the most common claims made by unsuccessful job applicants:

- Defamation: Defamation is one of the most popular tort claims in job reference cases. A defamatory job reference is one that makes false assertions of fact about the job applicant that causes a prospective employer to decline to hire the individual. For example, if a former employer knows that the applicant is fully literate, it should not report to the prospective employer that the applicant cannot read.[115]
- Emotional Distress: Unsuccessful applicants also might sue for intentional and/or negligent emotional distress. Emotional distress occurs when an employer acts in an outrageous manner with intentional or reckless disregard for the harmful emotional impact of that conduct on the job applicant.[116]
- Interference with Economic Advantage: Another legal claim is interference with prospective economic advantage. This claim asserts that the former employer interfered with the employment relationship being formed between the applicant and prospective employer.[117]
- Misrepresentation: It is a misdemeanor for a former employer to make false statements about former employees in an effort to prevent them from obtaining subsequent employment. Former employees may sue for treble or punitive damages as a civil remedy for misrepresentation.[118]

2. PRIVILEGED COMMUNICATIONS

Although the prospect of tort liability might be intimidating, Civil Code section 47(c) provides legal protection from liability for non-malicious job references, even if they are incorrect. Section 47(c) states that responses to prospective employers' requests for background information, made without malice, are privileged.[119] Civil Code section 47(c) expressly includes within the ambit of privileged communication references by prior employers. Section 47(c) provides that a privileged broadcast includes one made:

> *(c) In communication, without malice, to a person interested therein, (1) by one who is also interested, or (2) by one who stands in such a relation to the person interested as to afford a reasonable ground for supposing the motive for the communication to be innocent, or (3) who is requested by the person interested to give the information. This subdivision applies to and includes a communication concerning the job performance or qualifications of an applicant for employment, based upon credible evidence, made without malice, by a current or former employer of the applicant to, and upon request of, one whom the employer reasonably believes is a prospective employer of the applicant. This subdivision authorizes a current or former employer, or the employer's agent, to answer whether or not the employer would rehire a current or former employee.*

Thus, the issue is whether the former employer had credible information to support its statement to the prospective employer, and whether it acted with malice.

An employer should only give a reference if two criteria are met; 1) the reference is honest, and 2) the employer can prove it is honest. An employee may have been lazy, but if there is no performance evaluation, counseling memo, written warning or other documentation memorializing the employee's laziness, the employer will have a difficult time showing that it had credible information that will trigger the protection of section 47(c). If an employer has credible information to support a job reference, it will normally be protected from any civil tort claims.

Note that a waiver, while recommended, may not prove to be an absolute bar to liability.

McQuirk v. Donnelley[120]

The Ninth Circuit Court of Appeals interpreting California law, held that a County and its Sheriff were not immune from liability (despite a signed release) for providing a reference to a prospective employer for a former employee. Philip McQuirk was a former employee of the Glenn County, California Sheriff's Office. Five years after receiving a medical retirement from Glenn County, he applied for a non-peace officer position with the Mountlake Terrace Police Department in Washington State. McQuirk signed a release that authorized former employers to provide information regarding him, his work record, his reputation, and his financial status and waived liability for compliance. McQuirk, was hired on April 11, 1995. On April 12, 1995, Commander Smith of the Mountlake Terrace Police Department spoke with Louis Donnelley, Glenn County Sheriff, regarding McQuirk. McQuirk alleges that Donnelley made five defamatory statements about him during that conversation. McQuirk's offer was rescinded. McQuirk filed a lawsuit in Washington against Donnelley and Glenn County, seeking damages and injunctive relief for defamation. The Court granted the County's motion for summary judgment. McQuirk appealed.

The Court of Appeals reversed. Interpreting the law in the way it believed the California Supreme Court would, the Court held that pursuant to Civil Code Section 1668, the waiver signed by McQuirk was invalid as it improperly shielded Donnelley from liability for intentional torts. In addition, the Court held that Donnelley was not immune from liability under Government Code section 820.2, which supplies immunity for public officials for discretionary acts. The Court held that Donnelley's conduct in making the statements to McQuirk's prospective employer was a ministerial act, not discretionary. The Court concluded that section 820.2 confers immunity only with respect to basic policy decisions and found that the actions of Donnelley were on an operational level and not a planning/policy level. Similarly, the County would not be immune from liability. The Court noted, however, that Civil Code section 47(c) provides a qualified privilege for employers when giving references, and limited

its holding to prevent employers from prospectively contracting by waiver for more than the qualified privilege granted them under California law.

3. STATUTORY CLAIMS

State and Federal anti-discrimination laws prevent employers from taking adverse action - such as giving false job references - to individuals on the basis of a protected status. The law protects individuals on the basis of race, national origin, color, sex, sexual orientation, religion, disability, medical condition and numerous forms of protected activity. Examples of protected activity include seeking Workers' Compensation benefits, filing a discrimination or harassment complaint, and participating as a party or witness in a discrimination lawsuit.

Employers that give false job references because the current or former employee belongs to a protected class can be subject to significant liability under State and Federal anti-discrimination laws. As with tort claims, an employer sued for discrimination or retaliation under these laws must be able to prove that it gave an accurate reference. Documentation is therefore crucial. But proof of equal treatment is also important in discrimination cases. If an employer has a history of never providing job references, and it then provides an accurate, negative reference about a former employee with a protected status, a jury or court might find that the employer gave the reference because of the plaintiff's race, gender or other protected status. The employer's history of providing no reference could be enough to convince the jury or court that the employer would not have given any reference if the employee did not have the protected status. This could result in a judgment against the agency.

4. MANDATORY RESPONSE TO POLICE DEPARTMENT BACKGROUND INVESTIGATION

As discussed above, Government Code section 1031 requires law enforcement agencies to investigate whether peace officer applicants are fit to be peace officers. Section 1031.1 in turn requires current and former employers to disclose employment information to public safety departments conducting background checks. Employers must respond to requests for information if all of the following criteria are met:

- The candidate is not currently employed as a peace officer.
- The request is made in writing.
- The request includes a notarized authorization from the candidate releasing the employer from liability.

Do not forget the notarization requirement as this might invalidate the release. A peace officer or another authorized representative of the law enforcement agency must present the request and release from liability to the employer.

If these requirements listed above are met, the employer must provide any written information in its files about the applicant's employment and any other records relevant to peace officer performance. An employer is not required to provide a verbal reference, create any documents, or provide information that is protected from disclosure by law, i.e. employers should not release confidential references previously provided by third parties.

The Legislature has afforded former employers protection from liability for responses to police background investigations. Government Code section 1031.1 (b) provides, "in the absence of fraud or malice, no employer shall be subject to any liability for any relevant cause of action by virtue of releasing employment information required pursuant to this section."

5. DUTY TO MAINTAIN BACKGROUND CHECK INFORMATION

The EEOC requires institutions of higher education to preserve background information (application and other records) for two years after the record or an adverse action was taken, whichever is later, even if the person was not hired.[121] If a discrimination charge is filed, the records must be preserved until the case is concluded. The agency must use a secure method when disposing of the records.

6. RE-VERIFYING EMPLOYMENT ELIGIBILITY

Effective January 1, 2018, the Immigration Worker Protection Act (AB 450) prohibits a public or private employer, or a person acting on behalf of the employer, from re-verifying the employment eligibility of a current employee at a time or in a manner not required by Section 1324a(b) of Title 8 of the United States Code, unless otherwise required by federal law.[122] An employer who violates this provision is subject to a civil penalty of up to ten thousand dollars, except that the act will not also form the basis for liability or penalty for violating Labor Code section 1019.1.[123] This prohibition concerning re-verification is not meant to be interpreted, construed, or applied to restrict or limit an employer's compliance with a memorandum of understanding governing the use of the federal E-Verify system.[124] (See also Worksite Inspection of Personnel Files by Immigration Enforcement Agent, *infra*.)

SECTION 3 MEDICAL TESTING AND MEDICAL INFORMATION

A. APPLICABLE LAWS

In addition to the United States Constitution and the California Constitution discussed above in Section 1 of this workbook, many of the privacy issues regarding medical testing and medical information arise under provisions protecting employees from federal and state disability discrimination laws. While the focus of anti-disability discrimination laws is to prevent disability discrimination, they also protect individual privacy rights concerning applicant and employee medical information. Thus, they not only restrict the use of information about a disability, but also restrict the solicitation of such information. Due to the highly sensitive nature of employee medical information, the disability laws also require employers to strictly maintain the confidentiality of medical information. Additionally, Congress and the California legislature have also enacted statutes governing the handling and disclosure of medical information. This section provides an overview of these laws.

1. THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CMIA)

The Confidentiality of Medical Information Act (CMIA), California Civil Code sections 56-56.37, generally prohibits the acquisition, use and disclosure of medical information without prior written authorization from the person whom the information concerns. The CMIA also requires that medical records be kept confidential.

With limited exceptions, the CMIA prohibits an employer from using or disclosing (or knowingly permitting its employees or agents to use or disclose) medical information relating to an employee unless the employee first signs a valid authorization. For purposes of the CMIA, medical information is defined as,

> *"any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. 'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the person's name, address, electronic mail address, telephone number or social security number, or any information that, alone or in combination with other publicly available information, reveals he individual's identity."*[125]

2. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The Department of Human and Health Services (DHHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), PL 104-191, 110 Stat 1936, enacted regulations protecting medical information.

The federal regulations, entitled Standards for Privacy of Individuality Identifiable Health Information (Privacy Rule), protect individually identifiable health information of patients and, in some cases, employees. In particular, the Privacy Rule imposes standards regarding the rights of individuals who are the subjects of individually identifiable health information. The Privacy Rule also contains standards regarding the authorized and required uses and disclosures of this information by covered entities, and imposes several administrative burdens and onerous penalties for non-compliance.

3. THE FAIR EMPLOYMENT AND HOUSING ACT (FEHA)

The Fair Employment and Housing Act (FEHA), California Government Code sections 12900, et seq., generally prohibits employment discrimination on the basis of, among other things, an employee's physical/mental disability or medical condition. The FEHA is relevant in the context of a discussion of the confidentiality of medical records because it restricts the ability of employers to inquire about the medical condition and medical history of prospective and current employees. A violation constitutes an unlawful employment practice and may give rise to liability.[126]

4. THE AMERICANS WITH DISABILITIES ACT (ADA)

The Americans with Disabilities Act (ADA), 42 U.S.C. sections 12101- 12213, is the federal counterpart to the FEHA. Like the FEHA, it prohibits employment discrimination on the basis of a physical or mental disability. And, like the FEHA, it restricts the ability of employers to require prospective and current employees to undergo physical examinations as well as to inquire into their medical histories.

5. THE CALIFORNIA FAMILY RIGHTS ACT (CFRA)

The California Family Rights Act (CFRA), Government Code section 12945.2, requires a covered public employer to permit eligible employees to take a leave of absence of up to 12 weeks in a 12-month period for, among other things, the serious health condition of the employee or the employee's spouse, domestic partner, child or parent.

Under certain circumstances, the CFRA allows an employer to require an employee to produce medical certification of the serious health condition entitling the employee to leave as well as certification that an employee is capable of returning to work. The CFRA also contains provisions for maintaining the confidentiality of medical information.

6. THE FAMILY MEDICAL LEAVE ACT OF 1993 (FMLA)

The Family Medical Leave Act (FMLA), 29 U.S.C. section 2601, et seq., is the federal counterpart to the CFRA. Like the CFRA, the FMLA permits eligible employees to take a leave of absence of up to 12 weeks in a 12-month period for, among other things, the serious health condition of the employee or the employee's spouse, child or parent.

Likewise, the FMLA enables an employer, under certain circumstances, to require an employee to produce medical certification of the serious health condition entitling the employee to leave as well as certification that an employee is capable of returning to work.

7. THE CALIFORNIA OCCUPATIONAL SAFETY AND HEALTH ACT OF 1973 (CAL/OSHA)

The California Occupational Safety and Health Act of 1973 (Cal/OSHA), Labor Code §§ 6300-6719, regulates workplace health and safety conditions. It also contains provisions requiring the retention of certain medical and exposure records for up to 30 years.

8. THE OCCUPATIONAL SAFETY AND HEALTH ACT OF 1970 (OSHA)

The Occupational Safety and Health Act (OSHA), the federal counterpart to Cal/OSHA, 29 U.S.C. Sections 651-678, also regulates workplace health and safety issues.[127] It too requires the retention of certain medical and exposure records for up to 30 years.

9. PREGNANCY DISABILITY LEAVE (PDL)

The Pregnancy Disability Leave Act (PDL), Government Code § 12945, is a California law permitting women who are disabled as a result of pregnancy to take up to four months of unpaid leave in addition to the 12 weeks of leave provided under the CFRA. Similar to the CFRA and FMLA, the PDL authorizes an employer to require medical certification from an employee seeking leave.

10. CALIFORNIA LABOR CODE SECTION 3762

Section 3762 is applicable in workers' compensation proceedings. With limited exceptions, it prohibits a workers' compensation insurer, third party administrator or employee of a self-insured employer charged with administering workers' compensation claims from disclosing any medical information to an employer about an employee who has filed a workers' compensation claim.

11. GENETIC INFORMATION NONDISCRIMINATION ACT OF 2008 (GINA)

This law, codified at 42 U.S.C. section 2000ff-1(a), makes it an unlawful employment practice for an employer (employment agency, labor organization, or training program) to fail or refuse to hire, or to discharge, any employee, or to discriminate against any employee with respect to compensation, terms, conditions, or privileges of employment because of genetic information regarding the employee or to limit, segregate, or classify the employees of the employer in any way that would deprive or tend to deprive any employee of employment opportunities or otherwise adversely affect the status of the employee as because of genetic information of the employer.

Genetic information consists of:
Information about an employee's genetic tests or those of the employee's family member; or the manifestation of a disease or disorder in the employee's family members. Information about the sex or age of an individual is not considered genetic information.

Medical Information That is Not Genetic Information:
It shall not be a violation of this law to use, acquire, or disclose medical information that is not genetic information about a manifested disease, disorder, or pathological condition of an employee including a manifested disease, disease, disorder or pathological condition that may or may not have a genetic basis.

It is also an unlawful practice for an employer to request, require, or purchase genetic information with respect to an employee or an employee's family member, except where:

- the information was requested inadvertently;
- health services or genetic services are offered by the employer, including as part of a wellness program;
- the employee provides a prior knowing voluntary written authorization;
- an employer requests family medical history from the employee to comply with FMLA or applicable state laws;
- the information is publicly available (but not medical databases or court records);
- the information is to monitor the biological effects of toxic substances in the workplace; or
- the employer conducts DNA testing for law enforcement purposes but only to the extent that such genetic information is used for DNA markers to detect sample contamination.

Under the EEOC's final regulations regarding GINA, the inadvertent acquisitions of genetic information does not constitute a violation, such as in situations where a manager or supervisor inadvertently obtains employee genetic information through ordinary Internet searches or overhears a conversation. However, supervisors may not intentionally run a search or request information over a social networking site that is "likely to result in uncovering genetic information."[128]

Maintenance of Genetic Information:
If the employer possesses genetic information about an employee, such information must be maintained on separate forms and in separate medical files and must be treated as a confidential medical record of the employee.

Disclosure of Genetic Information:
Genetic information regarding an employee shall not be disclosed except:

- to the employee or employee's family members, at the written request of the employee;
- specified occupational or health research;
- in response to a court order;
- in compliance with FMLA;
- to a health agency pursuant to contagious disease outbreak.

Relationship to HIPAA:
This chapter does not prohibit a covered entity under HIPAA from any use or disclosure of health information that is authorized for the covered entity under such regulations. However, it is important to note that the March 26, 2013, modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules address the use of genetic information and prohibit health plans from using or disclosing genetic information for underwriting purposes, including plans to which GINA expressly does not apply. An exception to this prohibition exists for issuers of long-term care polices.[129]

12. California Consumer Privacy Act

The California Consumer Privacy Act of 2018 gives California residents ("consumers") the right to: (1) know what personal information a business has about them, and where information came from or was sent (e.g. who it was sold to); (2) delete personal information that a business collects from them; (3) opt-out of the sale of personal information about them; and (4) receive equal service and pricing from a business, even if they exercise their privacy rights under the law, with some exceptions.

Companies will need to provide information to consumers about these rights in privacy policies and will need to provide consumers with the ability to opt out of the sale of personal information by supplying a link titled "Do Not Sell My Personal Information" on their home page. The Act further provides that a business must not sell the personal information of consumers younger than 16 years of age without that consumer's affirmative consent or for consumers younger than 13 years of age, without the affirmative consent of the consumer's parent or guardian.

The Act defines "personal information" broadly as any information that identifies or can be used to identify a consumer or their household, such as: records of products purchased, browser search histories, educational information, employment history, and IP addresses.

Public entities do not need to comply because the law only applies to: for-profits doing business in California, that (a) have annual gross revenues in excess of $25 million; or (b) receive or disclose the personal information of 50,000 or more Californians; or (c) derive 50 percent or more of their annual revenues from selling California residents' personal information.

However, when contracting with covered companies, public entities will want to ensure that the obligations and risks of the law rest squarely with the for-profit business. Those risks are real. The Attorney General has enforcement authority over the Act. Consumers may bring class actions against non-compliant companies that allow sensitive consumer personal information to be stolen or wrongfully disclosed. In these cases, consumers may seek statutory damages between $100 and $750 per California resident per incident.

13. CALIFORNIA PATIENT PRIVACY PROTECTIONS

Due to an increase of employee snooping into celebrity medical files at UCLA, California laws are consistently evolving in an attempt to protect patient privacy. Health care providers must safeguard patient data and to report unauthorized access within five days to the state and the individual. The state can levy penalties up to $25,000 per patient for privacy breaches.

Section 1280.18 to the Health and Safety Code establishes the California Office of Health Information Integrity (CalOHII) to: (1) ensure the enforcement of state law mandating the confidentiality of medical information and; (2) impose administrative fines for the unauthorized access, use or disclosure of medical information.

Every provider of health care must establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information. Every provider of health care must also reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure.

"Unauthorized access" is defined as the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the CMIA or by other statutes or regulations governing the lawful access, use, or disclosure of medical information.

CalOHII shall also adopt, amend, or repeal such rules and regulations as may be reasonable and proper to carry out the purposes and intent of this division, and to enable the authority to exercise the powers and perform the duties conferred upon it by this division not inconsistent with any other provision of law.

The standards also apply to licensed health facilities. Section 1280.15 to the Health and Safety Code directs that "[a licensed] clinic, health facility, home health agency, or hospice...shall prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information...consistent with Section 130203."

Also, on August 19, 2009, pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, the U.S. Department of Health and Human Services (DHHS) issued "breach" notification regulations.[130] The regulations require health care providers and other covered entities under the Health Insurance Portability and Accountability Act (HIPAA) (see Section 3.J.3., *infra*.) to notify affected individuals following a breach of unsecured protected health information. If a breach occurs, covered entities must promptly notify affected individuals, the Secretary of DHSS, and in some cases, the media, of the breach. Minor breaches may be reported to the Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Pursuant to Section 1280.18(c), the department may conduct joint investigations of individuals and health facilities for violations of Section 1280.18 and Section 1280.15, respectively.

14. Adopting a Practical Approach

Complying with the various state and federal laws is not as difficult as it might first appear. It should be apparent after reviewing this workbook that state and federal laws on this topic are very similar and, in many instances, identical. Thus, compliance with state laws will very often equate to compliance with federal laws.

To the extent that there are differences between state and federal law, California law tends to impose greater restrictions on the acquisition, use and disclosure of medical information by employers. Thus, as a general rule, if an employer follows California law governing the acquisition, use and disclosure of medical information, the employer will meet or even exceed federal requirements.

Legal snapshot: Medical Testing and Medical Information	
Applicable laws:	• Constitutional Right of Privacy, Cal. Const. art. I, § 1 • Fair Employment and Housing Act (FEHA), Cal. Gov. Code §§ 12900, et. seq • American with Disabilities Act (ADA), 42 USC §§ 12101, et. seq. • Confidentiality of Medical Information Act (CMIA), Cal. Civil Code §§ 56, et. seq. • Health Insurance Portability and Accountability Act (HIPAA), 42 USC §§ 1301, et. seq. • Public Safety Officers' Procedural Bill of Rights Act, Cal. Gov. Code §§ 3300 *et seq.* • Genetic Information Nondiscrimination Act (GINA), 42 USC §§ 2000ff, et seq. • Various other California statutes • Common law torts
Who and what is protected?:	• Applicants and employees • Information about medical/psychological conditions

Generally, employers must NOT:	• Require medical tests or inquire about medical condition before making an offer • Require post-offer medical tests unless they are job-related and consistent with a business necessity, narrowly tailored, and uniformly applied. In addition, for pre-employment/ drug/alcohol tests, a "special need" must justify the test. • Base hiring or personnel decisions upon an applicant or employee's medical condition unless the applicant/employee is unable to perform the essential functions of the job, with or without reasonable accommodation • Disclose medical information about an applicant/employee absent written authorization, court order, or subpoena
Applicable balancing test:	• The interest of applicants and employees in keeping their medical condition and information private *v.* employer's legitimate need to determine whether applicant/employee is able to perform the essential functions of the job

B. PRE-OFFER INQUIRIES AND EXAMINATIONS — WHAT YOU CAN AND CANNOT ASK JOB APPLICANTS BEFORE MAKING A CONDITIONAL OFFER OF EMPLOYMENT

The pre-offer stage encompasses any hiring activity that occurs *prior to making a conditional offer of employment*, including but not limited to written job applications, employment interviews, background investigations, and decisions to hire. The following guidelines apply not only to questions directed to the applicant, but also apply to inquiries made of third parties about the applicant, such as the applicant's family, friends, and former employers. At this stage, an employer may not conduct a medical examination or make a "disability-related inquiry." Such an inquiry is defined "as a question [or a series of questions] that is likely to elicit information about a disability."[131]

1. WHAT IS A MEDICAL EXAMINATION?

An employer is prohibited under the ADA and FEHA from conducting a medical examination of a job applicant prior to a conditional offer of employment. According to the EEOC, a medical examination is a procedure or test that seeks information about an individual's physical or mental impairment or health.[132]

The EEOC has indicated that the following factors are helpful in determining whether a procedure or test is a medical examination:

- Is it administered by a health care professional?
- Are the results interpreted by a health care professional or someone trained by a health care professional?
- Is it designed to reveal an impairment of physical or mental health?
- Is it invasive (for example, does it require the drawing of blood, urine or breath)?
- Does it measure an applicant's performance of a task (permissible), or does it measure the applicant's physiological responses to performing the task (not permissible)?
- Is it normally given in a medical setting (for example, a health care professional's office)?
- Is medical equipment used?[133]

2. WHAT IS A CONDITIONAL OFFER OF EMPLOYMENT?

Under the FEHA and ADA, an employer's ability to ask questions about an applicant's medical condition and/or to require an applicant to undergo a medical examination depends primarily upon whether a conditional offer of employment has been made.

According to the EEOC, a conditional offer of employment is a job offer:

- that is made after the employer has evaluated all relevant non-medical information which could reasonably have been obtained and analyzed prior to making the offer; and
- conditioned upon acceptable medical information that is directly related to job performance and business necessity.[134]

If an employer is still waiting for the results of, for example, a criminal background check, an offer may not be considered a real conditional offer of employment. In the very limited case where an employer can show that it could not reasonably obtain and evaluate the non-medical information before a conditional offer was made, the EEOC would still consider it a real offer.[135] For example, it might be too costly for a law enforcement agency to administer two separate

polygraph tests – one before a conditional offer and the other after a conditional offer – so that it could ask medical questions during the polygraph test.[136] Another instance may be where an applicant requests that his or her current employer not be asked for a reference check until a conditional job offer is received. In that instance the potential employer would not be able to obtain the non-medical information (reference check) until the offer is made.[137]

LCW Practice Advisor

An employer faces a steep burden to prove it could not have obtained and analyzed non-medical information prior to making a conditional offer of employment. Once a conditional offer has been made, if the employer is still waiting for non-medical information, the employer should attempt to obtain and evaluate that information prior to conducting any medical examinations or inquiries.

3. CASE STUDY ON CONDITIONAL OFFER OF EMPLOYMENT

Leonel v. American Airlines [138]

Three HIV positive individuals applied to American Airlines for flight attendant positions. After providing written applications and participating in phone interviews, American flew them to the company's headquarters for in-person interviews. After the interviews, American extended a conditional offer of employment that was conditioned on the results of a background investigation and medical examination. Immediately after making the conditional offers, American representatives directed them to go to American's medical department for medical examinations. The applicants were required to provide a medical history and blood and urine samples for testing.

Despite questions which would have revealed whether they were HIV positive, none of the applicants disclosed that they were HIV positive or that they were taking medications for their condition. However, a blood test revealed that the applicants were HIV positive. As a result, American sent letters to the applicants stating that the conditional offers were being withdrawn. The letters explained that the applicants did not fulfill all conditions in that they "failed to be candid or provide full and correct information." The applicants sued for violations of the ADA, the FEHA and their constitutional right to privacy.

American argued that its hiring process was legal since the company first evaluated the non-medical information and only then considered the applicants' medical condition. The Ninth Circuit disagreed, holding that medical information cannot be collected or analyzed until after all non-medical information has been evaluated, unless the non-medical information could not reasonably have been obtained. The Court noted other procedures that American could have utilized to complete the background checks prior to the medical exams, such as completing

the background checks before the applicants arrived, flying the applicants back at a later date for their medical exam or having the medical exams performed by regional medical sites or the applicants' own doctors. However, the Court did not actually rule that American violated the statutes but rather remanded the case to the District Court for a determination of whether American Airlines can prove that it could not reasonably have completed the background checks prior to initiating the medical exams.

LCW Practice Advisor

If an employer wants to obtain or analyze non-medical information after a conditional offer has been made, the employer will have to prove that it could not have reasonably obtained that information prior to making the conditional offer. In that situation, after the conditional offer the employer should still attempt to obtain and analyze all of the non-medical information before obtaining medical information.

4. ACCEPTABLE PRE-OFFER INQUIRIES

A job applicant may be asked to describe or demonstrate how, with or without reasonable accommodation, the applicant will be able to perform job-related functions.[139] For example:

- "This job requires that you to be able to lift 50 pounds, can you do that?"
- "What are your qualifications and skills?"
- "Do you ever use illegal drugs?"[140]
- "Can you meet our attendance requirements?"

5. EXAMPLES OF IMPROPER PRE-OFFER INQUIRIES

It is unlawful to include general questions regarding disability status on an application form or pre-employment questionnaire or in the course of the selection process.[141] Under the ADA and FEHA, an employer may not do the following in the pre-offer stage:

- conduct a medical examination of the applicant and/or inquire about the applicant's medical background;
- test for alcohol;[142]
- ask whether an applicant has a disability; or
- ask an applicant about the nature or severity of his or her disability.[143]

For example, at the pre-offer stage, an employer cannot ask direct or indirect questions that are likely to elicit information about a disability, such as the following:

- "Do you have any particular disabilities?"
- "Do you need a reasonable accommodation to perform the job duties?"
- "How serious is your medical condition?
- "Have you ever been treated for any of the following diseases and conditions?"
- "Do you take any medication?"
- "How did you become disabled?"
- "Are you now receiving or have you ever received Workers' Compensation?"
- "How often will you need to get treatment?" [144]

6. PHYSICAL AGILITY/FITNESS TESTING

Under the ADA and the FEHA, applicants may be required to undergo physical agility/fitness testing if it is directly related to job performance and is consistent with a business necessity.[145] For many public employees, physical fitness is not a consideration. But, in some cases, particularly in the case of safety employees (e.g., police and fire), physical fitness is an important consideration. In such cases, physical agility testing may be appropriate.

Although medical inquiries are not permitted until after a conditional offer has been made, an employer may ask an employee to have a physician certify whether he or she can safely perform a required physical agility test.[146] The applicant may obtain a note stating that he or she can safely perform the test, or explain the reasons why he or she cannot perform the test.[147] The employer is not entitled to review the applicant's entire medical file or obtain medical information not affecting the ability of the applicant to perform the test safely.[148]

LCW Practice Advisor

- Tests that measure the applicant's physiological or biological responses would constitute a prohibited medical examination because they measure the body's physiological response as opposed to measuring the applicant's ability to perform certain tasks
- Since an employer cannot inquire about an applicant's medical background prior to making a conditional offer of employment, an employer who is administering a physical agility/fitness exam should strongly consider advising participants of the components of the exam and the physical stresses involved before the exam is

administered. By doing so, an employer may avoid or reduce liability where an applicant injures himself or herself in the course of physical fitness/agility testing.

7. DRUG AND ALCOHOL TESTING OF APPLICANTS

The Ninth Circuit Court of Appeals held in *Lanier v. City of Woodburn* (9th Cir. 2008) 518 F. 3d 1147, 1152, that employers must have a "special need" to require pre-employment drug testing. Please refer to section 4 of this workbook for a detailed discussion of drug and alcohol testing.

8. PSYCHOLOGICAL TESTING

Under California law, employers are also prohibited from requiring a psychological examination prior to making a conditional offer of employment.[149] Under the ADA, if the psychological test is "medical," i.e., if it provides evidence that would lead to identifying a mental disorder or impairment, the test is prohibited. However, under the ADA, a test that measures personality traits such as honesty, preferences, and habits would not be considered a medical examination.[150]

C. HOW TO HANDLE THE OBVIOUSLY DISABLED APPLICANT

Sometimes an applicant's disability will be obvious to an employer (e.g., the applicant is missing a limb). In such circumstances, the employer may still inquire about the applicant's ability to perform the essential functions of the job. The employer may also ask an applicant with a known disability to demonstrate how he or she would perform an essential function of the job. The employer may also ask the applicant whether he or she requires a reasonable accommodation to perform the job and what type of accommodation is required.[151]

> *However, the EEOC has indicated that where an applicant discloses a disability or the disability is otherwise obvious, the employer should not inquire further into the nature or severity of the disability (e.g., "How did you lose your leg?")*[152]

Also, if the known disability would not interfere with the performance of a job-related function, then the employer cannot ask the applicant how he or she would perform the job unless all applicants are asked the same question.[153] (e.g., the applicant is seeking a job as a typist and has a prosthetic leg).

D. POST-OFFER MEDICAL EXAMINATIONS AND INQUIRIES

After making a conditional offer of employment, an employer may, with certain limitations, obtain medical or psychological information about an applicant's ability to perform essential job functions.[154]

1. REQUIREMENTS FOR POST-OFFER MEDICAL EXAMINATIONS

An employer may condition an offer of employment on the results of a medical examination, which is conducted prior to the start of employment, for purposes of determining fitness for the job in question if:

- all entering employees in the same job classification are subjected to such an examination;
- an applicant or employee may submit independent medical opinions for consideration before a final determination on disqualification is made, if the results of such medical examination would result in disqualification; and
- the results are maintained on separate forms and be accorded confidentiality as medical records.[155]

Under the ADA, employers are afforded wide latitude in making general inquiries about an applicant's medical background or disability status. According to the EEOC, "[o]nce a conditional job offer is made the employer may ask disability-related questions and require medical examinations as long as this is done for all entering employees in that category. If the employer rejects the applicant after a disability-related question or medical examination, investigators will closely scrutinize whether the rejection was based on the results of that question or examination."[156]

However, under the FEHA, an employer may inquire about an applicant's medical condition and/or require a medical examination, but may never make general inquiries into an applicant's medical background, disability status, etc. All such inquiries and/or examinations must always be directly related to the job in question and consistent with business necessity.[157]

LCW Practice Advisor

This is an area where California law is more restrictive than federal law. *Under California law, any request for information or examination must be job-related and consistent with business necessity*. The ADA permits more general inquiries into an applicant's medical condition than does the FEHA. Thus, even if an employer complies with the provisions of the ADA, the employer may be violating the FEHA. Employers should be particularly careful about using standardized employment applications and questionnaires that were not created to comply with California law.

2. HIV TESTING IS IMPERMISSIBLE

California employers are generally prohibited from testing applicants and employees for HIV and from basing hiring and employment decisions on such tests.[158]

E. EXISTING EMPLOYMENT STAGE: THOSE WHO ARE ALREADY EMPLOYED

The threshold for testing individuals who are already employees is much higher. One reason is that employers have the opportunity to observe existing employees' ability to function in their jobs, unlike applicants.[159] Thus, the general rule is that an employer may not inquire about an existing employee's medical condition or require a current employee to undergo a medical examination.[160] However, there are two primary exceptions: 1) to carry out a legal obligation, such as determining the availability of a reasonable accommodation; and 2) for other nondiscriminatory, legitimate business reasons, such as determining an employee's fitness for duty. Like pre-employment medical exams, exams of existing employees must also meet the job-related and consistent with business necessity requirements.[161]

F. DENIAL OF EMPLOYMENT BASED ON MEDICAL EXAMINATION RESULTS

If an employer disqualifies an applicant based on a medical examination, the employer must show that: 1) the reasons for disqualification were job-related and consistent with business necessity; and 2) no reasonable accommodation was available.[162] (See Section 4 regarding Reasonable Accommodation). An employer must engage in an interactive reasonable accommodation discussion to determine if a reasonable accommodation exists. If the results of a medical examination result in disqualification, an applicant may submit an independent medical opinion for consideration before a final determination on disqualification is made.[163]

1. EMPLOYERS MAY REJECT APPLICANTS WHOSE JOB PERFORMANCE WOULD ENDANGER THE APPLICANT OR OTHERS

The FEHA and the ADA have similar but distinct tests regarding the rejection of applicants whose medical condition or disability endangers the applicant or others.

a. The ADA "Direct Threat" Test

Under the ADA, an employer may refuse to hire an applicant who poses a direct threat to the health or safety of the applicant or other individuals in the workplace. "Direct threat" means a significant risk of substantial harm to the health or safety of the individual or others that cannot be eliminated or reduced by reasonable accommodation. The determination that an individual poses a "direct threat" should be based on an individualized assessment of the individual's present ability to safely perform the essential functions of the job. This assessment should be based on a reasonable medical judgment that relies on the most current medical knowledge and/or the best available objective evidence. In determining whether an individual would pose a direct threat, the factors to be considered include:

- The duration of the risk;
- The nature and severity of the potential harm;
- The likelihood that the potential harm will occur; and
- The imminence of the potential harm.

b. The FEHA "Safety-of-Others" Test

Similar to the ADA's "direct threat" test, the FEHA permits an employer to refuse to hire an applicant if the applicant, because of his or her disability or medical condition, cannot perform the job's essential duties without endangering the health or safety of the applicant or the health or safety of others even with reasonable accommodations. However, unlike the ADA, the FEHA distinguishes between the threat posed to the applicant and the threat posed to others. Disqualification based upon the threat to an applicant requires an employer to show that the job imposes an imminent and substantial degree of risk to the applicant that cannot be cured by reasonable accommodation.[164]

The FEHA "safety-of-others" test applies a much more lenient standard for an employer to disqualify an applicant. Rather than showing an imminent threat, an employer need only show that the person would endanger the health or safety of others to a greater extent than if an individual without a disability performed the job.

2. CASE STUDY ON FEHA "SAFETY-OF-OTHERS" TEST

***Equal Employment Opportunity Commission v. United Parcel Service, Inc.*[165]**
Defendant United Parcel Service, Inc. ("UPS"), denied driving positions to certain employees because the employees failed to pass UPS's "Vision Protocol," which requires drivers to have some central vision and some peripheral vision in each eye. The employees alleged that UPS had discriminated against them because of their monocular vision, a disability, in violation of the FEHA. The Ninth Circuit found that the employees were sufficiently limited in the major life activities of seeing and working to fall within the FEHA's broad definition of disability.

However, the court ruled in favor of UPS because UPS had demonstrated that the employees would "endanger the health or safety of others to a greater extent than if an individual without a disability performed the job" and, thus, had satisfied FEHA's safety-of-others defense. The court noted that even a modest increase in the risk that a problem will occur is significant when the potential consequences of that problem are very serious. The court also emphasized that peripheral vision plays an important role in avoiding accidents and that the monocular driver has less opportunity to see a child or any other pedestrian or cyclist or car darting from the impaired side. Finally, the court held that UPS

demonstrated that decreased peripheral vision compromises a driver's ability to perform safely as compared to a person without that impairment.

3. CASE STUDY ON PRE-EMPLOYMENT MEDICAL EXAMINATIONS

***Norman-Bloodsaw v. Lawrence Berkeley Laboratories*[166]**
Present and former employees, who, as applicants, submitted to a medical examination following a conditional offer, brought suit alleging a violation of the ADA and the right to privacy under the United States and the California Constitutions alleging that the tests performed were neither job-related nor required by business necessity. In the course of the pre-employment physical examinations, the applicants completed medical history questionnaires and provided blood and urine samples. The questionnaires asked, among other things, whether they had ever had any one of approximately 61 medical conditions including, but not limited to, sickle cell anemia, venereal disease and, in the case of women, menstrual disorders. In addition, the blood and urine samples were tested for syphilis. Blood samples provided by African-American applicants were also tested for sickle cell trait and blood samples provided by female applicants were tested for pregnancy. The applicants and employees alleged that the testing for syphilis, sickle cell trait, and pregnancy occurred without their knowledge or consent, and without any subsequent notification that the tests had been conducted.

The Ninth Circuit found for the applicants as to their constitutional claims in ruling that that the scope of the physical extended beyond the reasonable expectations of an occupational health exam, as the employer tested for intimate medical conditions bearing no relationship to their job duties or working conditions as clerical employees.

G. CURRENT EMPLOYEES

The general rule is that an employer may not inquire about a current employee's medical condition or require a current employee to undergo a medical examination.[167] There are, however, several very important exceptions to this rule, such as fitness for duty examinations (discussed in Section 6), and an employee's request for a reasonable accommodation.

LCW Practice Advisor

A fitness for duty examination or inquiry into a request for reasonable accommodation must be job-related and consistent with business necessity.[168]

1. REQUESTS FOR REASONABLE ACCOMMODATION

Under both the FEHA[169] and the ADA, an employer must make reasonable accommodation for a qualified employee with a disability.[170] Accordingly, an employer may make limited inquiries to verify an employee's need for a reasonable accommodation.

Under the ADA, an employer may require an employee to undergo a medical examination if the employee requests a reasonable accommodation. According to the EEOC, when an employee requests a reasonable accommodation (and his or her disability is not obvious) an employer may request "reasonable documentation" concerning the employee's alleged disability.[171]

Under the FEHA, an employer may request an employee to submit to a physical examination if the request is directly related to the ability of the employee to perform his or her job and a business necessity.[172] Thus, an employer could require an employee to undergo a physical examination if the employee requests a reasonable accommodation.

a. What Does "Reasonable Documentation" Mean?

Under the ADA, "reasonable documentation" means that the employer may require only the documentation needed to establish that a person is disabled and that the disability necessitates a reasonable accommodation.

In response to a request for reasonable accommodation, an employer cannot ask for documentation that is unrelated to determining the existence of a disability and the necessity of an accommodation. In most situations an employer cannot request a person's complete medical record because it is likely to contain information unrelated to the disability at issue and the need for accommodation. If an individual has more than one disability, an employer can request information pertaining only to the disability that requires a reasonable accommodation.

There is no California regulation or statute which directly addresses this question *in the context of the FEHA*. However, under the CMIA (discussed at greater length below), an employer would be entitled to the same information (i.e., certification that the employee is disabled and information concerning any reasonable accommodation that may be required). Under the CMIA the employer is only entitled to information describing the functional limitations of the employee that may entitle the employee to leave or limit the employee's fitness to perform his or her present employment. No statement of medical cause should be included in the information disclosed.[173]

b. Choosing a Doctor

Under the ADA, an employer may require an employee to go to an appropriate health professional of the employer's choice if the employee provides insufficient information from his/her treating physician to substantiate that he/she has a disability and needs a reasonable accommodation. *However, the EEOC recommends that an employer give an employee an opportunity to provide additional information that may be needed before sending the employee to a physician of the employer's choosing*.[174]

Documentation from an employee is considered insufficient if it does not specify the existence of an ADA disability and/or explain the need for reasonable accommodation.[175]

c. Obvious Disabilities

If an employee's disability is obvious, then the employer may not require the employee to obtain medical certification of the disability. But, the employer may still request certification that the employee's disability does not pose a risk to himself or herself or other employees.

d. A Promotional Candidate Is Treated as an Applicant

According to guidance provided by the EEOC, an employer should treat an employee who applies for a new job within the agency as an applicant. The employer, therefore, is prohibited from asking disability-related questions or requiring a medical examination before making the individual a conditional offer. Moreover, any medical examination required for a promotion would have to be job-related and consistent with business necessity. Unless the position involves significantly different duties than the applicant's current position, an employer will have a hard time justifying the business necessity of a promotional medical examination. Note also that an individual is not an applicant where he or she is noncompetitively entitled to another position with the same employer (i.e., because of seniority or satisfactory performance in his or her current position). Likewise, an employee who is temporarily assigned to another position and then returns to his or her position is not an applicant.[176]

Finally, an employer generally will not be able to conduct a suspicionless drug test on an employee who seeks a promotion, absent a unique requirement in the new position.[177]

2. REQUESTS FOR MEDICAL LEAVE UNDER THE FMLA AND CFRA

Under both the FMLA and CFRA, an employer may request medical certification for purposes of establishing an employee's entitlement to a medical leave as a result of the serious health condition of an employee or an employee's child, spouse, or parent.[178] The FMLA recognizes spouses as individuals in either same sex or common law marriages.[179] Effective January 1, 2020, registered domestic partners can be any couples, regardless of their sex. Domestic partners are also covered by the CFRA but not by the FMLA.

Certification is defined as a written communication to the employer from the health care provider of the employee or the employee's child, parent, domestic partner or spouse.[180]

a. What Is a Serious Health Condition?

A serious health condition means a physical or mental condition that involves either:

- inpatient care in a hospital, hospice, or residential health care facility; or
- continuing treatment or continuing supervision by a health care provider.[181]

b. Certification of an Employee's Own Serious Health Condition

Under the CFRA, if the certification pertains to the employee's own serious health condition, the certification must contain:

- the date, if known, on which the serious health condition commenced;
- the probable duration of the condition; and
- a statement that, due to the serious health condition, the employee is unable to work at all or is unable to perform the function of his/her position.[182]

Under the FMLA, essentially the same information is required. However, under the FMLA, the employer is entitled to know the medical facts which support the certification.[183] An employer cannot ask an employee to furnish information beyond that requested in the DFEH form.[184]

LCW Practice Advisor

California employers should only utilize the DFEH form –not the DOL form– for purposes of certification of entitlement to CFRA and FMLA leaves because the DFEH form does not contain a space for the health care provider to disclose the underlying medical facts or diagnosis of the serious health condition involved without the consent of the patient.[185] In this way, California employers will not receive confidential information that they are not entitled to receive.

c. Certification of a Parent, Spouse, Domestic Partner or Child's Serious Health Condition

Under the CFRA, if the certification regards the serious health condition of the employee's parent, spouse, domestic partner or child, then the certification must contain:

- the date, if known, on which the serious health condition commenced;
- the probable duration of the condition;
- an estimate of the amount of time the health care provider believes that the employee needs to care for the parent, child, spouse or domestic partner; and
- a statement that the serious health condition warrants the participation of the employee to provide care during a period of treatment or supervision of the parent, child, spouse or domestic partner.[186]

The serious health condition of a parent, spouse, domestic partner or child "warrants the participation of the employee" when the employee is needed to provide psychological comfort, to arrange third party care or to provide or participate in the provision of medical care.[187]

Under the FMLA, the certification should contain the same information.[188] Note that domestic partners are not covered under the FMLA.

d. Recertification

Under the CFRA, the employer may require that the employee obtain subsequent recertification regarding the employee's serious health condition if additional leave is required.[189]

Furthermore, upon the expiration of the time estimated by the health care provider to be necessary for the care of a parent, spouse, domestic partner or child, the employer may require the employee to obtain recertification.[190]

Under the FMLA, recertification may be required on a "reasonable basis." According to federal regulations, unless "the employer receives information that casts doubt upon the employee's stated reason for the absence" or "circumstances described by the previous certification have changed significantly (e.g., the duration or frequency of absences, the severity of the condition, complications)," it is unreasonable to request recertification more often than every 30 days (or, if the length of leave specified in the original certification was greater than 30 days, prior to the expiration of the original leave).[191]

e. Getting a Second Opinion

Under both the FMLA and CFRA, if an employer doubts the validity of a certification provided by an employee, the employer may require, at the employer's expense, that the employee obtain the opinion of a second health care provider of the employer's choosing.[192]

> ***Please note:*** *The health care provider may not be employed by the employer (e.g., a county should not send an employee to its own health department to get a second opinion).*[193]
>
> *If the second opinion differs from the first opinion, the employer may require, again at the employer's expense, that the employee obtain an opinion from a third health care provider designated or jointly approved by the employer and the employee.*[194]

The third opinion is binding on the employer and the employee.[195]

f. Certification of an Employee's Ability to Return to Work

Absent a contrary position in a memorandum of understanding (or collective bargaining agreement), an employer may have a uniformly applied practice or policy that requires an employee to obtain certification from his or her health care provider that the employee is able to resume work if the employee is returning from leave taken as a result of his or her own serious health condition.[196] State law allows an employer to condition an employee's return to work from his or her own serious health condition upon a return to work certification only if the employer has a uniformly applied practice or policy of requiring such releases from all employees who return to work from illness, injury or disability.[197]

LCW Practice Advisor

While an employer may request certification of an employee's ability to return to work, the employer may not condition return to duty upon a certification that the employee can return to work without any restrictions. To do so would violate the duty of reasonable accommodation under the ADA and the FEHA.

3. CERTIFICATION OF ENTITLEMENT TO PREGNANCY LEAVE

An employer may require medical certifications before permitting employees to take a leave of absence under the PDL, or to transfer to a different position because of pregnancy, childbirth or other related medical conditions, *if it requires certification of other similarly situated employees, i.e., other employees seeking leave for medical reasons.*[198]
The certification should include the following information, and nothing else:

- The date on which the employee became disabled due to pregnancy, childbirth, or related medical conditions;
- The probable duration of the period or periods of disability; and
- An explanatory statement that, due to the disability, the employee is unable to work at all or is unable to perform any one or more of the essential functions of her position without undue risk to herself, the successful completion of her pregnancy, or to other persons.[199]

If the certification contains the above information, the employer must accept it as sufficient.[200]

An employer may also require an employee returning to work from pregnancy disability leave to obtain a release to return to work stating that the employee is able to resume her original job duties. However, the employer may only require a release if the employer has a uniformly applied practice or policy of requiring such releases from other similarly situated employees returning to work after a non-pregnancy related disability leave.[201]

4. WORKERS' COMPENSATION

This workbook is not intended to address workers' compensation issues. However, employers should be aware of some of the restrictions on the acquisition of medical information that exist in that context.

An employer generally may not receive medical information from an insurer about an employee who files a workers' compensation claim:

"An insurer, third party administrator retained by a self-insured employer…and those employees and agents specified by a self-insured employer to administer the employer's workers' compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in subdivision (b) of Section 56.05 of the Civil Code, about an employee who has filed a workers' compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers' compensation is claimed and the treatment provided for this condition (2) Medical information regarding the injury for which workers' compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee's work duties."[202]

5. DRUG TESTING OF CURRENT EMPLOYEES

The ADA does not encourage, prohibit, or authorize testing for the illegal use of drugs or making employment decisions based on such test results. The FEHA does not address drug testing.

However, the ability of public employers to test for illegal drug usage is limited by the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable searches and seizures, and by an employee's right to privacy. Please refer to Section 4 for a detailed discussion concerning the circumstances under which a government employer may require a drug test.

H. FITNESS FOR DUTY EXAMINATIONS

This section outlines the authority of an employer to require a current employee to undergo medical and/or psychological examinations for purposes of determining the employee's "fitness for duty."

<u>*Under the ADA and the FEHA*</u>, an employer may require an employee to undergo a medical examination (and/or inquiry) if it is job-related and consistent with business necessity.[203] According to the Interpretive Guidance issued by the EEOC, the above rule permits employers to require a fitness for duty exam, when there is a need to determine whether an employee is still able to perform the essential functions of his or her job.[204]

Moreover, the courts have upheld a public employer's right to conduct fitness for duty examinations. In the words of the Ninth Circuit Court of Appeals:

"The government clearly has a valid concern with the productivity and stability of its work force. Citizens rightly expect the government to operate as effectively and efficiently as it can, given the diverse tasks with which it is charged. The

government cannot operate with any degree of efficiency if its employees miss work…. Regular performance of [an employee's] work is a prerequisite for… most if not all full-time governmental jobs."[205]

1. When Is a Fitness for Duty Examination Allowed?

According to the Ninth Circuit Court of Appeals, "when health problems have had a substantial and injurious impact on an employee's job performance, the employer can require the employee to undergo a physical examination designed to determine his or her ability to work, even if the examination might disclose whether the employee is disabled or the extent of any disability."[206]

The Sixth Circuit Court of Appeals has stated the test this way: "for an employer's request for an exam to be upheld, there must be significant evidence that could cause a reasonable person to inquire as to whether an employee is still capable of performing his job."[207]

LCW Practice Advisor

A good rule of thumb to follow is not to request an employee undergo a fitness for duty examination unless you have specific evidence: 1) that an employee has difficulty performing one or more essential functions of his or her job; or 2) of other good cause (i.e., excessive absenteeism, poor productivity).

2. When Is a Fitness for Duty Examination Required?

In limited circumstances, the law may even mandate fitness for duty examinations. Indeed, the EEOC's Interpretive Guidance recognizes that the ADA permits periodic physicals to determine fitness for duty or other medical monitoring if such physicals or monitoring are required by medical standards or requirements established by federal, state, or local law.

Examples

- OSHA requires that employees exposed to certain hazardous substances be periodically monitored.[208]
- OSHA requires that employees who wear respirators must undergo a medical examination to ensure that the employee may safely wear a respirator.[209]
- Mandated drug testing for employees who operate commercial vehicles.[210]
- *California Government Code* § 1031(f) requires that peace officers be free from any physical, mental or emotional condition that might adversely affect their exercise of peace officer powers.

3. CASE STUDIES ON FITNESS FOR DUTY EXAMINATIONS

Yin v. State of California[211]
A state tax auditor with a five-year history of egregious absenteeism and on-the-job illnesses sued California to enjoin the state from requiring her to undergo a fitness for duty medical examination. After years of excessive absenteeism, the supervisor requested to see a copy of the employee's medical records. When she refused, she was asked to submit to an independent medical examination. The employee retained a lawyer and the State dropped its request. However, the absences continued and the state again demanded an independent medical examination. The employee then filed suit.

The Ninth Circuit Court of Appeals upheld the employer's right to require a medical examination where the exam was job-related and the record clearly indicated good cause for trying to determine whether she was able to perform her job in light of missing an excessive number of workdays. The employee's excessive absenteeism had seriously impacted her productivity and overall job performance. In this case, Yin's expectation of privacy was diminished and requiring her to undergo a fitness-for-duty examination would clearly further the state's interest in assuring a productive and stable work force.

Deckert v. City of Ulysses[212]
An insulin-dependent diabetic police officer was properly required to submit to a fitness for duty examination where the requirement was based upon sudden poor job performance and erratic behavior by the officer. After 17-years as a police officer, the officer's job performance suddenly plummeted. He left his patrol car unlocked, unattended and running while responding to a call, resulting in an individual parking it several blocks away. He also failed to write a required report on a domestic violence call, failed to provide backup for a building search by two other officers, and failed to lock his patrol car at the end of his shift. On the basis of these deficiencies and his inadequate investigation of a tire theft two months earlier, the police chief suspended him, demoted him from sergeant, and required him to undergo a medical exam to determine if his suddenly poor duty performance was caused by diabetes. The Court upheld the examination based on the officer's poor performance, and the City's actions which were consistent with the ADA and sound management principles.

***Fritsch v. City of Chula Vista*[213]**
A city attorney was properly required to undergo a psychiatric evaluation after she appeared visibly shaken, was hyperventilating and in a state of frenzy while in court. The supervisor relayed these observations to a consulting psychiatrist who confirmed the need for the evaluation. The attorney challenged the examination in court. The court upheld the employer's need to conduct a fitness for duty examination based on "the information available to the employer about the severity of the outburst and his personal observations of the attorney's demeanor when she reported the incident; the staff psychiatrist's recommendation that the employee immediately take a fitness-for-duty evaluation; and the high level of fortitude and professionalism required of litigation attorneys."

***Jermon v. County of Sonoma*[214]**
A janitor came to work and locked himself in the employee break room. After discovering him, his supervisors ordered him to take a fitness for duty examination for drug or alcohol abuse. The employee brought suit challenging the county's policy. The county's fitness for duty drug and alcohol policy required the following procedures: 1) the employee exhibit at least two conditions commonly associated with substance abuse, 2) the supervisor check with their manager prior to testing, 3) the supervisor talk with the employee regarding their behavior, 4) the supervisor speak with medical staff regarding the behavior, 5) the supervisor must keep records of all suspected behavior and 6) the employee must be returned to work if he or she is found to be "fit." The court upheld the policy in finding no constitutional violations or evidence that the testing was a condition of employment.

4. WHAT INFORMATION IS AN EMPLOYER ENTITLED TO RECEIVE FOLLOWING A FITNESS FOR DUTY EXAMINATION?

Under the Confidentiality in Medical Information Act (CMIA), unless written authorization is received from an employee, an employer is only entitled to know whether the employee can perform the essential functions of the job. The employer cannot be advised of the medical cause of an employee's inability to perform.[215]

If an employee requires a reasonable accommodation or is otherwise unable to perform the essential functions of the job, the employer is entitled to know the functional limitations on the employee's ability to perform the job (e.g., the employee cannot stand for extended periods of time; the employee cannot lift objects weighing more than 25 pounds).[216] If there is any doubt, an employer should not be afraid to seek clarification from the examiner concerning what an employee can and cannot do.

5. WHAT INFORMATION CAN THE EMPLOYER GIVE A DOCTOR?

Unless a health care professional is regularly called upon to treat a specific group of employees (e.g., a police department may regularly send officers to a particular physician for fitness for duty examinations), he or she may not have the requisite knowledge of a position to know what the essential functions of the job are, let alone make a determination that an employee can or cannot perform those functions.

The solution to this problem is simple. Nothing in the law prohibits an employer from providing a health care provider with a detailed job description, or even an opportunity to visit the job site to see how the job is performed.

I. CAN THE DOCTOR HAVE AN EMPLOYEE'S PRIOR MEDICAL RECORDS?

In some instances a health care provider will indicate that he or she needs to review the employee's prior medical records to conduct an effective fitness for duty examination. Under the CMIA, the health care provider cannot have the records unless the employee authorizes the release except under certain limited conditions.[217]

Civil Code section 56.20, subdivision (b), provides that:

> *"No employee shall be discriminated against in terms or conditions of employment due to that employee's refusal to sign an authorization under this part. However, nothing in this section shall prohibit an employer from taking such action as is necessary in the absence of medical information due to an employee's refusal to sign an authorization under this part."*

For example, if an applicant refuses to sign the authorization, the employer need not process the application. Likewise, if an employee refuses, the employer may discipline the employee for his or her performance.

J. HANDLING AND MAINTENANCE OF EMPLOYEE MEDICAL INFORMATION

Employee medical and psychological information is understandably accorded greater protection than many other types of employee information.

1. REQUIREMENTS REGARDING EMPLOYEE MEDICAL FILE

California law requires an employer, including a public employer, who receives medical information to establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information.[218] This includes any information regarding an individual's mental condition.[219] The procedures must include, but need not be limited to, instructing employees and agents on properly handling files containing medical information to protect the confidentiality of the information.[220]

The Americans with Disabilities Act (ADA), [221] also requires that information obtained regarding the medical condition or history of an employment applicant be kept confidential with few exceptions. The ADA further requires that information from medical examinations or inquiries be placed in a separate file and not placed in an employee's general personnel file.[222]

2. CONFIDENTIALITY OF MEDICAL INFORMATION ACT

a. What Is "Medical Information" for Purposes of the CMIA?

The CMIA defines medical information as:

> *"any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."*[223]
>
> *Medical information is "individually identifiable" if it "includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity."*[224]

b. Requirements of Valid Authorization

A health care provider cannot release information to an employer (or anyone else for that matter) unless the patient's written authorization:

- Identifies the person authorized to release the information;
- Identifies the person authorized to receive the information;
- Identifies any limitations on the types of information to be disclosed and the purposes for which the information can be used;
- *States a specific date after which the health care provider is no longer authorized to disclose the information;*

- Is typed or handwritten by the person signing it;
- Is separate from any other language contained on the same page and executed by a signature that serves no other purpose; and
- Advises the signing party of the right to receive a copy of the authorization.[225]

c. Exceptions to the Rule—Instances When Written Authorization Is Not Required under the CMIA

There are several exceptions to the requirement of written authorization that are relevant in the employment context.

- Medical information shall be disclosed by a health care provider in the course of legal proceedings pursuant to a subpoena or order of the court, board, commission, or other administrative body having jurisdiction of the matter and legal authority to compel the production of records.

Also, a health care provider may exercise its discretion to disclose medical information to an employer without written authorization if:

- ❑ the employer is responsible for paying for health care services rendered to the patient and it is necessary to disclose the records to the employer to allow the employer to determine responsibility for payment; or
- ❑ the information pertains to health care services which were rendered to an employee at the request and expense of the employer; and
    - the information is relevant to a lawsuit or other legal proceeding to which the employer and employee are parties and the employee has placed his or her medical history, mental or physical condition, or treatment at issue; or,
    - the information is limited to a description of the functional limitations of the patient that may entitle the patient to leave from work for medical reasons or limit the patient's fitness to perform his or her present employment and provided that no statement of medical cause is included in the information disclosed.[226]

d. A Memorandum of Understanding—A Possible Exception to the Exceptions

If an employer has adopted a written policy or has entered into a memorandum of understanding that provides that certain types of medical information shall not be used or disclosed by the employer in particular ways, the employer must obtain an authorization for those uses or disclosures even if it would not otherwise be required by the CMIA.[227]

3. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Privacy regulations enacted by the Department of Human and Health Services (DHHS) under the Health Insurance Portability and Accountability Act (HIPAA), Title 42 United States Code section 1301 *et seq*.

The primary thrust of HIPAA's Privacy Rule is directed at hospitals, doctors, medical clinics, health plans and health insurers. However, under some circumstances, local public agencies may be subject to the Rule's requirements as well.

Covered entities under HIPAA are health plans, health care clearinghouses or health care providers conducting certain health care transactions electronically.[228] Also affected by HIPAA are hybrid entities whose business activities include both covered and non-covered functions,[229] and health plan sponsors.

Public employers are covered entities under two specific circumstances:

- First, if the public agency provides health care to the general public by means of a hospital, clinic or any similar method of delivering health care, it is a covered entity. Significantly, the providing of paramedic services through a Fire Department may subject the agency's paramedic functions to HIPAA's Privacy Rule.
- Second, if the public agency has a self-administered health plan with 50 or more participants it is subject to HIPAA. Self-insured plans, cafeteria plans or flexible spending accounts with more than 50 participants (if administered by a public agency rather than a third-party administrator) are all covered by HIPAA.

If a public agency has an outside administrator for its health plans, cafeteria plans or flexible spending accounts, then it is not covered by the full range of HIPAA's Privacy Rule. However, even if it is not a covered entity, a public agency still has to meet certain lesser requirements such as:

- Ensuring that the third party administrator is complying with the Privacy Rule;
- Obtaining authorizations from employees to access information about their health claims
- Ensuring that the health plan provides that employees can access their own health information.

HIPAA's Privacy Rule imposes a number of administrative requirements on covered entities. If your agency is a covered or hybrid entity, the Rule requires it to do the following:

- Notify individuals regarding their privacy rights and how their protected health information (see Section J.3.a.iv.c. below) can be used or disclosed.

- Adopt and implement internal privacy policies and procedures.
- Train employees to understand these policies and procedures as appropriate for their functions in carrying out duties related to the employer's capacity as a health plan or health provider.
- Designate individuals who are responsible for implementing these policies and procedures, and who will receive privacy-related complaints.
- Establish privacy requirements in contracts with business associates that perform functions related to the employer's capacity as covered entity.
- Implement appropriate administrative, technical, and physical safeguards to protect the privacy of health information, so that it is not readily available to those who do not need it.
- Meet obligations concerning the exercise by individuals of their rights under the Privacy Rule.[230]

An agency must designate an employee to serve as the privacy officer. HIPAA does not specify any particular qualifications, but an employer should consider selecting someone with knowledge of the agency as a whole from a management perspective and a familiarity with benefits administration.

Additionally, covered entities must require business associates to comply with HIPAA's Privacy Rule. A business associate is a person or entity that performs certain functions on behalf of a covered health plan or health care provider which involve the use or disclosure of information protected by HIPAA's Privacy Rule. Examples of functions carried out by business associates include claims processing, quality assurance, and billing. Although HIPAA does not regulate business associates, a covered entity that contracts with a business associate must require that the business associate comply with HIPAA's Privacy Rule. Use and disclosure by business associates of information protected under HIPAA's Privacy Rule is further described below.

K. DISCLOSING MEDICAL INFORMATION

As previously noted, under the CMIA the general rule is that an employer may not disclose medical information unless written authorization is obtained from the subject employee.[231] Exceptions to the rule requiring written authorization include:

- when disclosure is compelled by judicial or administrative process or by any other specific provision of law;
- when the information is relevant to a lawsuit, arbitration, grievance or other proceeding to which the employer and employee are parties and the employee has placed his or her medical history, mental or physical condition or treatment at issue;

- administering and maintaining employee benefit plans, including health care plans and plans providing short-term and long-term disability income, and workers' compensation; or
- when the employee is incapacitated and the information is necessary to aid the treatment or diagnosis of the employee (See section 5 and 6).

The following are some specific types of requests for medical information that employers might receive.

1. EMPLOYEE REQUESTS

California Labor Code section 1198.5 gives employees the right to inspect their personnel files.

Government Code section 3306.5 gives public safety officers the right to inspect their personnel files.

California Government Code section 31011 gives county employees the right to inspect their files.

Education Code section 87031 gives employees of community college districts the right to inspect their personnel files pursuant to California Labor Code section 1189.5.

Under CalOSHA, it appears that whenever an employee who is exposed to toxic or harmful substances requests access to medical or "exposure" records, the employer shall assure that access is provided in a reasonable time, place and manner, but in no event later than 15 days after the request for access is made.[232]

2. RESPONDING TO SUBPOENAS

a. State Tribunals

With the exception of workers' compensation proceedings, California law requires that consumers and employees be given notice and an opportunity to object if certain records about them, including but not limited to medical and employment records, are subpoenaed.[233]
A party subpoenaing medical records must notify the consumer whose records are being sought at least 5 days prior to service of the subpoena upon the records custodian. Additionally, the notice to the consumer must be served on the consumer at least 10 days prior to the date of production.[234] The party subpoenaing records must also serve the responding party (i.e., the employer) with proof that the employee has been given notice of the subpoena. Unless the employer receives proof that the employee has been properly notified at least five days prior to service of the subpoena on the employer, the employer should not produce any records.

An employer may also contest a subpoena, by filing a motion to quash the subpoena.

b. Federal Tribunals

The *Federal Rules of Civil Procedure* do not impose the same notice requirements. Upon receipt of a subpoena for records, an employer must serve written objections to the subpoena on the grounds that the records are confidential within 14 days of being served with the subpoena, or prior to the date for compliance if the compliance date is less than 14 days. The objections must specify the grounds for the objections and describe the confidential records sufficiently to enable the subpoenaing party to move to compel their production.[235] Having served objections to the subpoena, the employer is not obligated to produce the records unless and until ordered to do so by the court. In the alternative, the employer may also move to quash the subpoena on the same grounds.[236]

c. Public Records Request

The California Public Records Act (CPRA)[237] makes a wide variety of government records available to the public. However, there are also a number of records that are not subject to disclosure such as "personnel, medical or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy."[238]

Also, the CPRA should be interpreted in light of the CMIA which requires, as indicated above, written authorization from the patient before medical records can be released.

It is recommended therefore that medical records not be released pursuant to a public records request. Nonetheless, the party submitting the request should be notified within 10 days of the decision not to comply with the request and the reasons therefore.[239]

d. Peace Officer Personnel Records

Peace officer personnel records demand special attention. Peace officer personnel records, including the medical records of a peace officer, are confidential[240] and may only be disclosed pursuant to a noticed motion (known as a *Pitchess* motion), and then only after an in camera review is conducted by the court.[241]

The only instances when a *Pitchess* motion is not required for discovery of peace officer personnel records are: 1) when the officer requests to review his or her own records, 2) pursuant to a subpoena in federal court proceedings or 3) in the course of an investigation by a grand jury or the district attorney into peace officer misconduct.[242]

On September 30, 2018, Governor Edmund G. Brown, Jr. signed Senate Bill 1421 and Assembly Bill 748 that will allow members of the public to obtain certain peace officer personnel records that were previously available only through the *Pitchess* procedure by making a request under the CPRA as described above.

Senate Bill 1421

Effective January 1, 2019, SB 1421 amends Government Code Section 832.7 to generally require disclosure of records and information relating to the following types of incidents in response to a request under the CPRA:

> Records relating to the report, investigation, or findings of an incident involving the ***discharge of a firearm at a person*** by a peace officer or custodial officer.
>
> Records relating to the report, investigation or findings of an incident in which the ***use of force*** by a peace officer or custodial officer against a person results in ***death or great bodily injury***.
>
> Records relating to an incident in which a ***sustained finding*** was made by any law enforcement agency or oversight agency that a peace officer or custodial officer engaged in ***sexual assault involving a member of the public***. "Sexual assault" is defined for the purposes of section 832.7 as the commission or attempted initiation of a sexual act with a member of the public by means of force, threat, coercion, extortion, officer of leniency or any other official favor, or under the color of authority. The propositioning for or commission of any sexual act while on duty is considered a sexual assault.
>
> Records relating to an incident in which a ***sustained finding*** of ***dishonesty by a peace officer or custodial officer*** directly relating to the reporting, investigation, or prosecution of a crime, or directly relating to the reporting of, or investigation of misconduct by, another peace officer or custodial officer, including but not limited to, any sustained finding of perjury, false statements, filing false reports, destruction of evidence or falsifying or concealing of evidence.

NOTE*: Several police labor organizations have taken the position* Section 832.7 *was not intended to apply retroactively to records that are in an agency's possession but were created before January 1, 2019. This question is the subject of multiple parallel lawsuits across the state. Rulings have come in from three superior courts: Contra Costa Superior Court denied six police unions' petitions to limit disclosures to records created after January 1; Ventura County Superior Court issued a preliminary injunction that prevents the County from releasing records of pre-2019 incidents, and Los Angeles County Superior Court concluded that there was no legislative intent to preclude pre-2019 records. As each of these rulings come from the Superior Courts, they are not binding except for the parties to each case. LCW has a designated team of attorneys closely following developments in the new law and we will continue to post updates on our blog as they occur. This law will likely remain unsettled until there is a ruling from either a Court of Appeal of the California Supreme Court.*

Assembly Bill 748

AB 748 requires agencies, effective July 1, 2019, to produce ***video and audio recordings*** of "critical incidents," defined as an incident involving the ***discharge of a firearm*** at a person by a peace officer or custodial officer, or an incident in which the ***use of force*** by a peace officer or custodial officer against a person resulted in ***death or great bodily injury***, in response to CPRA requests.

These statutes have different timelines for production of records, and different circumstances under which production of records can be delayed or records can be withheld. Further, agencies may wish to evaluate their document retention policies in light of these new disclosure requirements. Agencies should work closely with trusted legal counsel to ensure compliance with both statutes.

e. *Inquiries by Prospective Employers*

Under the CMIA, written authorization from the employee is required before medical information could be disclosed to a prospective employer. In light of the legal restrictions placed upon the acquisition of medical information concerning prospective employees, an employer should be wary of such requests. Thus, in the absence of written authorization, medical information should not be provided.

3. CASE STUDIES INVOLVING DISCLOSURE OF MEDICAL INFORMATION

Garrett v. Young[243]

A patient sought medical treatment for a rash, sleeplessness, weight loss, and complained of stress. The doctor diagnosed her with severe depression, referred her to a psychiatrist, and sent "return-to-work" documents to her employer. After inquiry from the employer, the doctor indicated that the patient suffered from itching and stress. The doctor did not discuss any diagnostic tests nor did he reveal the psychiatric referral. After discovering that the doctor had disclosed some information to her employer, the plaintiff brought suit alleging a violation of the CMIA.

Both the trial and appellate court found no violation of the CMIA as the patient's rash and itching were plainly visible. Moreover, she had discussed her condition, along with job-related stress, to co-workers, thereby waiving her right to sue for a violation of the CMIA. In addition, an employer that receives a document from a medical doctor purporting to contain a medical excuse for failure to appear at work may verify its contents with the physician whose name appears on it without either party violating the CMIA. A health care provider is statutorily permitted to discuss "a general description of the reasons for treatment, the general nature of the injury or condition, [and] the general condition of the patient," as this doctor did. This plaintiff failed to provide a specific, written request to the health care provider to prevent release of information.

***Pettus v. Cole*[244]**
Plaintiff was required to submit to a medical examination by an employer-selected doctor in order to receive short-term disability for stress. The initial doctor referred the plaintiff to a psychiatrist, who after suspecting alcohol abuse, then referred plaintiff to a third doctor who specialized in chemical dependency. Both subsequent doctors failed to obtain written authorization from the employee to disclose information to his employer. Nonetheless, both psychiatrists provided detailed written and oral reports to his employer. Both doctors disclosed details about the employee's work and family history, his drinking habits, his problems at work, his violent thoughts towards a co-worker, and his current psychiatric symptoms. Both doctors also told the supervisor that they thought the employee was using alcohol "adversely." Based on the above information, the employer directed the employee to enroll in a 30-day inpatient alcohol treatment program, and when the employee refused, his employment was terminated.

The employee brought suit alleging a violation of CMIA and invasion of right to privacy. The court found for the employee against both the physicians and employer. A physician may only disclose the functional limitations of the employee. The employer also violated the CMIA by acting on the improperly obtained medical information. The physicians and employer also invaded the employee's reasonable expectation of privacy, without a compelling interest to justify such intrusion.

***Shaddox v. Bertani*[245]**
A dentist reported suspected prescription drug abuse by a police officer to the officer's employer. The dentist had originally prescribed Vicodin following the removal of the officer's wisdom teeth. Months later, the officer became irate after the dentist refused to renew the prescription. The dentist reported the behavior to the police department, which initiated an investigation and disciplined the officer for "improper conduct." The officer sued alleging a violation of the CMIA.

The dentist's disclosure was permitted under the CMIA since a state statute directed agencies that employ peace officers to establish a procedure to investigate complaints by members of the public.

SECTION 4 DRUG AND ALCOHOL TESTING AND INFORMATION

Drug and alcohol testing, like general medical testing, is subject to restrictions that protect an employee's right of privacy. In this area, the employee's interest is in the freedom to engage in off-duty conduct, but employers have a strong interest in maintaining a safe and drug-free workplace. Drug and alcohol abuse testing programs, especially those implemented by public employers, have become a common source of litigation. One reason is that public employers, unlike private sector employers, are subject to constitutional restrictions regarding privacy and due process. Testing programs, especially if carelessly or unfairly administered, can also result in tort liability for defamation, invasion of privacy, assault and battery, or intentional infliction of emotional distress. Thus, it behooves every employer to develop a clear, even-handed drug policy that not only assures a drug-free work environment but adequately considers an employee's right to privacy.

A word of caution: many of the legal issues involved in this area are still being defined by the courts. Consequently, employers are strongly advised to consult with counsel in order to keep abreast of changes in the law.

Legal snapshot: Drug/Alcohol Testing and Information	
Applicable laws:	• Constitutional Right of Privacy, Cal. Const. art. I, § 1 • Fair Employment and Housing Act (FEHA), Cal. Gov. Code §§ 12900, *et. seq* • American with Disabilities Act (ADA), 42 USC §§ 12101, *et. seq*. • Confidentiality of Medical Information Act (CMIA), Cal. Civil Code §§ 56, *et. seq*. • Health Insurance Portability and Accountability Act (HIPAA), 42 USC §§ 1301, *et. seq*. • Public Safety Officers' Procedural Bill of Rights Act, Cal. Gov. Code §§ 3300 *et seq*. • Various other California statutes • Common law torts
Who and what is protected?:	• All applicants and employees • Information about drug and alcohol use
Generally, employers must NOT:	• Require pre-employment drug/alcohol tests unless a "special need" justifies the test. In addition, the tests must be job-related and consistent with a business necessity, narrowly tailored, and uniformly applied • Require drug/alcohol testing of existing employees unless there is reasonable suspicion • Disclose drug and alcohol testing information about an applicant/employee absent written authorization, court order, or subpoena
Applicable balancing test:	• Applicant's/employee's interest in keeping off-duty conduct private *v.* Employer's legitimate interest in and obligation to provide a safe and drug-free work environment

A. EMPLOYER-REGULATED DRUG AND ALCOHOL TESTING

1. GENERAL LEGAL STANDARDS

In 1997, the California Supreme Court, in *Loder v. City of Glendale*, ruled that drug and alcohol testing of all applicants for public employment who have been given conditional offers of employment is constitutionally permissible, but that drug and alcohol testing for all current employees who apply for promotions within a public agency is not.[246] The 2008 decision of the Ninth Circuit in *Lanier v. City of Woodburn* (9th Cir. 2008) 518 F.3d 1147, however, has called into question the continued validity of *Loder*. In *Lanier*, the Ninth Circuit held that a public employer must demonstrate a "special need" to justify suspicionless pre-employment drug tests of job applicants. *Loder* involved the validity of the City of Glendale's blanket drug and alcohol testing program under which all applicants for positions with the City, as well as all current City employees who had been approved for promotion to new positions were required to undergo urinalysis testing. *Lanier* involved a preemployment drug testing policy that the City of Woodburn, Oregon applied to all applicants for City employment, and specifically limited its application to positions for which no "a special need" for drug testing was shown.

Leonel v. American Airlines Inc.[247] illustrates why the sequence of background investigations, medical examinations and drug testing in the hiring process can be a trap for the unwary employer. In *Leonel*, three HIV positive individuals applied to American Airlines for flight attendant positions. After providing written applications and participating in phone interviews, American flew them to the company's headquarters for in-person interviews. After the interviews, American extended a conditional offer of employment that was conditioned on the results of a background investigation and a medical examination (which included a drug test). Immediately after making the conditional offers, American representatives directed them to go to American's medical department for medical examinations. The applicants were required to provide a medical history and blood and urine samples for testing.

Despite questions which would have revealed whether they were HIV positive, none of the applicants disclosed that they were HIV positive or that they were taking medications for their condition. However, a blood test revealed that the applicants were HIV positive. As a result, American sent letters to the applicants stating that the conditional offers were being withdrawn. The letters explained that the applicants did not fulfill all conditions in that they "failed to be candid or provide full and correct information."

The three rejected applicants sued American alleging that its practice of conducting the medical examination (which included the drug test) before completing the background investigation violated the ADA and the FEHA. Specifically, they argued that it was illegal for American to refuse to hire them for not disclosing their HIV positive status and HIV related medications because a "real" conditional job offer had not been properly made before American obtained medical information from them.

The Ninth Circuit Court of Appeals noted that the ADA and the FEHA not only bar discrimination against disabled applicants, but also regulate the sequence of employers' hiring processes. Specifically, these statutes prohibit medical examinations and inquiries until after the employer has made a "real" job offer to an applicant.[248] A "real" job offer under the ADA and FEHA means that the employer must have evaluated all "non-medical" information or be able to demonstrate that it could not reasonably have done so before making the conditional offer. By withholding medical information until the last stage of the hiring process, applicants can determine whether they were rejected because of disability or because of insufficient skills or bad references.

Under the ADA, testing designed solely to determine the current use of illegal drugs is not considered a "medical examination."[249] Similarly, the FEHA does not treat the current use of illegal drugs as a disability, and nothing in the FEHA or any other California statute prohibits or otherwise limits testing for illegal drugs.[250] If drug testing is not a medical examination, it would need to be performed pre-offer unless the test could not reasonably be performed pre-offer. Many employers test applicants for drugs that might be legal under some circumstances but could also impair an employee's job performance, such as prescription medications like Vicodin. Since the use of legal drugs or alcohol could be considered to be a medical examination, testing for those substances may only be performed after a conditional offer has been extended.[251]

Whether drug testing is performed pre or post conditional offer, the EEOC is of the opinion that employers may ask follow-up questions about an applicant's lawful drug use after an applicant tests positive for illegal drug use.[252] However, it is generally preferable to require an applicant to identify any substances that might result in a positive drug test before conducting the drug test, so that the applicant cannot later fabricate an explanation for the positive drug test. Moreover, the FEHA specifically prohibits any medical inquiry before a conditional offer has been made. Thus, if an employer wishes to conduct an effective drug test, the employer will likely need to conduct that test after a conditional offer has been made.

In the post-*Leonel* world, an employer should carefully plan the sequence of its hiring processes, including drug testing. An employer should also carefully consider which drugs are going to be screened in its drug tests. An employer that tests for drugs that could impair an employee's job performance, but could also have legitimate lawful uses, such as Vicodin, will likely need to conduct the drug test after a conditional offer of employment has been made. If the employer is testing solely for drugs that are illegal under any circumstances, the testing can be performed before a conditional offer of employment is made.

a. Pre-Employment, Conditional Offer Stage

Pre-employment drug testing may be an effective means of deterring drug user applicants from applying for a position as well as detecting drug users who do apply. Because the consumption of alcohol is legally permissible, most employers do not specifically want to deter an applicant who consumes alcohol from applying for employment. However, a policy of conducting tests allows employers to obtain notice of potential alcohol abusers.

Currently, however, the testing of applicants is permissible at this stage only upon a showing of a "special need." In *Lanier* the Ninth Circuit Court of Appeals reasoned that notwithstanding the public entity's interest in addressing a generalized societal drug use problem, pre-employment, suspicionless drug testing violates a job applicants' Fourth Amendment protection against unreasonable searches and seizures unless the entity can demonstrate that the particular position is safety-sensitive and involves a danger to the public. In *Lanier*, the plaintiff applied for a job as a page with the City of Woodburn's public library. She accepted a conditional offer for the position subject to her successful completion of a background check and pre-employment drug and alcohol testing. She refused to take the drug test and the city rescinded its job offer. The Ninth Circuit held that the city's drug testing policy was not unconstitutional on its face because the city could require applicants for certain positions to take a drug test. However, the court held that the city's policy was unconstitutional as applied to Lanier and the library page position because no "special need" was shown to justify the testing.

The court in Lanier explained that the public entity there was unable to make a substantive showing of how drug abuse within the city affected job performance in the past. In addition, there was no evidence that library pages cared for children or were in a position to exert influence over children. The mere presence of children in the library was insufficient to justify suspicionless drug testing of all applicants. In contrast, the court recognized that school teachers and school administrators can be drug tested prior to employment because of their direct role in children's lives and because of the obvious social interest in protecting children. Finally, the court held that the library page position was not safety-sensitive merely because it had been characterized as such in the city's internal policies and procedures manual.

Safety-sensitive positions are those jobs where individuals perform work that involves a danger to the public. The following are examples of jobs previously found to pose a danger to the public: operating railway cars, operating dangerous instrumentalities such as heavy trucks used to transport hazardous material, work regarding national security, work in a nuclear power facility, work in the aviation industry, work involving the enforcement of drug laws and operating natural and liquefied natural gas pipelines.

In order to avoid privacy violations and illegal search claims, employers should take care to identify those positions for which there exist a "special need" for pre-employment drug testing. Employers should inform applicants for these positions that their pre-employment physical examination will include a drug and alcohol screen. It is probably not sufficient notice if applicants are merely aware that blood or urine tests will be conducted. Specific written notice should be provided at the beginning of the application process. Notice of such testing can best be accomplished through a written consent form given at the start of the application stage. An employer should also give the applicant a copy of its drug and alcohol policy. Of course, the results of the medical examination and test on which the employer conditions an offer of employment must remain confidential and must be kept on forms that are separate from the applicant's other records.

b. Existing Employment Stage

The *Loder* court concluded that the City of Glendale's practice of conducting a drug and alcohol test on all applicants for promotion (i.e., individuals who were already employed by the City), without regard to the nature of the position sought, violated the Fourth Amendment to the federal Constitution, which guarantees freedom from unreasonable searches and seizures. This aspect of the *Loder* decision appears to remain in effect notwithstanding the Ninth Circuit decision in *Lanier* which did not involve review of the public entity's drug testing policy as to those already employed.

The court determined that the reasonableness of such testing depends on the nature and duties of the promotional position, and that such testing would be appropriate only for safety and security sensitive positions. The reason given for treating applicants for initial employment differently than applicants for promotion was that an employer does not have an opportunity to observe applicants over a period of time but can observe its employees to evaluate whether they abuse drugs and/or alcohol.

Bases for reasonableness of testing existing employees is covered in more detail below in other sections of this workbook.

c. Off-Duty Drug Use Issues

Employees may complain that drug and alcohol testing allegedly allows employers to intrude on the employees' "recreational" off-duty use of these substances. However, this will usually not occur if employers require testing only upon reasonable suspicion that the particular employee is under the influence of drugs or alcohol *on the job*. In this way, the focus is not on the employee's off-duty conduct, but rather the impact of drug used on the employee's work performance and workplace safety.

Employers can minimize potential privacy right violations in the following ways:

- ❑ Implement the drug and alcohol policy fairly, reasonably, and in the least intrusive manner.
- ❑ Notify and provide each employee covered by the policy with a copy of the drug and alcohol policy.
- ❑ Explain the policy to each employee.
- ❑ Avoid penalizing an employee for his or her off-duty conduct unless such conduct can be shown to affect the employee on the job.
- ❑ Conduct all discussions, interviews and tests in private areas to maintain confidentiality.
- ❑ Always act professionally, courteously and in a non-accusatorial manner.
- ❑ Maintain confidentiality of all documentation.

***Edgerton v. State Personnel Board*[253]**
A Caltrans equipment operator failed a random drug test by testing positive for marijuana. The employee was suspended and agreed to remain drug free and to submit to random drug testing. Subsequently, the employee was given an off duty drug test where he tested positive for methamphetamines. After he was terminated, the employee filed a suit in state court alleging that off-duty drug testing infringed upon his right to privacy. The court issued an injunction prohibiting Caltrans from conducting off-duty drug testing of its employees. Caltrans appealed and the appellate court affirmed the decision. The court stated that the intrusion into an individual's privacy is significantly enhanced when the employee is subject to follow-up drug testing on his off-duty time. Moreover, Caltrans failed to explain why follow-up drug testing could not instead take place during an employee's regular work hours.

2. TYPES OF DRUG TESTING FOR EXISTING EMPLOYEES

a. The "Reasonable Suspicion" Standard

The Fourth Amendment to the United States Constitution protects individuals from unreasonable intrusions by government officials; this includes unreasonable drug testing. However, in *Skinner v. Railway Labor Executives' Association*, the United States Supreme Court upheld drug testing of any railroad employee where there was reasonable suspicion of impairment due to drug use.[254] After *Skinner*, courts have held that drug and alcohol testing of employees is legally permissible when there is some individualized basis for suspecting that an employee is currently using illegal drugs and/or alcohol, and that such use has impaired the performance of his or her job duties.

b. Objective Evidence Required

Although reasonable suspicion testing does not require certainty, mere "hunches" are not sufficient to meet this standard. The criteria justifying reasonable suspicion include the following:

- Observable phenomena, such as direct observation of drug use or possession and/or the physical symptoms of being under the influence of a drug;
- A pattern of abnormal conduct or erratic behavior;
- Arrest or conviction for a drug-related offense, or the identification of an employee as the focus of a criminal investigation into illegal drug possession, use or trafficking;
- Information provided either by reliable and credible sources or independently corroborated; or
- Newly discovered evidence that the employee tampered with a previous drug test.[255]

Examples of observable phenomena or abnormal conduct may include the following kinds of objective indicators:

- Bloodshot eyes
- Slurred speech
- Alcohol odor on breath
- Unsteadiness in walking
- An accident involving employer property
- Physical altercation
- Verbal altercation
- Behavior that is so unusual that it warrants summoning a supervisor, manager or someone else for assistance
- Possession of substances in violation of the employer's drug and alcohol policy
- Information obtained from a reliable person with personal knowledge

These are not the exclusive indicators for determining reasonable suspicion. The number of reasonable suspicion indicators and the compelling nature of the evidence attached to each indicator will determine whether the employer had sufficient reasonable suspicion to test. Consequently, any one indicator above or in combination with other indicators will not necessarily indicate reasonable suspicion. Each situation will have to be individually examined, but obtaining as much evidence of impairment as possible can only strengthen an employer's case. Thus, before requiring an employee to submit to a drug and/or alcohol test, the employer should gather as much evidence as possible and document in writing the specific facts and rational inferences from these facts which reasonably warrant suspicion that the particular employee to be tested is under the influence of drugs or alcohol.

Courts consider the following factors when balancing the employer's interest in testing against the employee's privacy interests:

- Past, documented problems/accidents resulting from drugs and/or alcohol;
- The risk of safety hazards from impaired employees upon the public;
- Exposure of covered employee to a criminal element and controlled substance;
- The required carrying of a firearm by covered employees;
- Access to truly "sensitive" information;
- Diminished privacy expectations of covered employees;

- That employees work in an industry which traditionally has been highly regulated; and
- The manner in which the test is given (no surgical intrusion, advance notice of testing given, no physical observation of providing urine specimen).

United Teachers of New Orleans v. Orleans Parish School Board,[256]
The Fifth Circuit Court of Appeals held that a school district may not subject its employees to drug testing simply because they were injured on the job, as that policy violates the protection against unreasonable searches and seizures under the Fourth Amendment of the United States Constitution. This case involved two Louisiana school districts with a policy that subjected all teachers, aides and clerical workers who are injured on the job to drug testing. Under the policy there was no requirement that the injury occur under circumstances suggesting drug use was involved. The teachers' union filed a lawsuit in federal court to enjoin the policy. The United States District Court for the Eastern District of Louisiana refused to enjoin the drug testing. The teachers appealed. The Court of Appeals reversed. The court held that the policy violates the Fourth Amendment guarantee against unreasonable searches and seizures because the policy does not require that there be a suspicion of drug use related to the injury. The court held that there must be adequate individualized suspicion of wrongful drug use to require testing.

c. Permissible Testing in the Absence of Reasonable Suspicion

In March 1989, the United States Supreme Court carved out two significant exceptions to the individualized "reasonable suspicion" standard.

i. Employees Involved with Drug Interdiction or Who Carry Firearms

First, in *National Treasury Union v. Von Raab*,[257] the court approved drug testing of employees as a condition of transfer or promotion into positions that are directly involved in the interdiction of illegal drugs or who are required to carry firearms in the line of duty because such employees have a diminished expectation of privacy in respect to the intrusions occasioned by a urine test. The court found a sufficient governmental interest in ensuring that front-line drug interdiction personnel are physically fit, free of drug use and have unimpeachable integrity and judgment. The court also found that the public interest demands effective measures to prevent promotion or transfer of drug users into positions requiring the employee to carry firearms. Those positions may demand the use of deadly force. The risk of death or injury to members of the public is great, so that even a momentary loss of attention can have disastrous consequences.

The court did not specifically address the issue of whether or not employees *currently* occupying positions involved in drug interdiction and requiring the carrying of firearms could be tested for drugs. The holding implies, however, that the court would approve such tests because it recognizes that this class of public employees have a "diminished" expectation of privacy. If an agency can show the necessity of such tests to protect the public and assure successful

performance of safety functions, the extent of governmental interest may well outweigh the intrusion into the privacy of employees in those limited positions. It would be important, however, for the agency to make that particular showing. Otherwise, testing of currently employed personnel should only occur if there is reasonable suspicion as outlined above.

ii. Post-Accident Testing

The second exception to the individualized "reasonable suspicion" standard allows testing of employees following certain accidents if an employer can show a history of severe accidents related to drug or alcohol abuse, or if it can prove that there is catastrophic risk to the public unless certain employees are drug-free and able to devote constant and uninterrupted attention to their jobs. In *Skinner v. Railway Labor Executives*,[258] the United States Supreme Court approved post-accident blood and urine testing, without individualized suspicion, of railway workers in the following circumstances:

- immediately following a train accident involving a fatality,
- release of hazardous materials accompanied by an evacuation,
- a reportable injury or damage to railroad property of $500,000.00 or more, or
- collision resulting in a reportable injury, or in damage to railroad property of $50,000 or more.

An employer, therefore, may be able to justify post-accident testing of employees without a showing of individualized suspicion. However, it would be necessary to show a history of drug/alcohol abuse and/or a high risk of danger to the public. Any post-accident testing procedures should be carefully tailored to follow the basic principles set out in *Skinner.*

Excluding one of the two limited circumstances discussed above, employers may not test employees without reasonable suspicion.

Inadequate History or Catastrophic Risk

A California court found the post-accident drug testing of employees in the Office of Personnel Management (OPM) unlawful in the absence of reasonable suspicion.[259] OPM's policy provided for testing whenever there was an on-duty accident that required hospitalization or caused property damage over $1,000.00. The court distinguished this drug testing plan from the one approved in *Skinner* in that in the OPM policy, a much lower threshold damage amount permitted drug testing ($1,000, compared to at least $50,000 in *Skinner*). The court also noted that the OPM did not make a showing of a past history of drug/alcohol abuse, as the railroad did in *Skinner*. Moreover, the court found that the risk of harm to the public in the event of accident by an impaired OPM worker to be "trivial" compared with the potential for catastrophic harm associated with an impaired railway worker controlling a train.

d. Random Drug Testing

Courts have taken varying views of random drug testing, usually upholding random drug testing of employees in safety-sensitive positions, but invalidating random testing of other employees.

Smith v. Fresno Irrigation District,[260]
A California court upheld the random testing of employees in safety sensitive positions involving heavy equipment, and agency vehicles. The court further considered the impact of the employees' performance, reflexes, and judgment on the safety of others.

American Federation of Labor v. Unemployment Insurance Appeals Board[261]
A California court held that a random drug test of a worker on an offshore oil drilling rig did not violate the California constitutional right to privacy due to the hazardous nature of the offshore platform which gave the employer a compelling interest in maintaining a drug-free workplace. Also, the employee had a reduced expectation of privacy because he knew when he took the job that he could be tested at any time.

AFGE v. Roberts[262]
The Ninth Circuit Court of Appeals upheld random drug testing of correctional officers. In doing so, the court found that the government's interest in preventing drug use by prisoners and maintaining an alert security force outweighed the privacy interests of the officers.

International Brotherhood of Teamsters v. Department of Transportation[263]
The Ninth Circuit Court of Appeals upheld Federal Highway Administration's random drug testing for drivers of commercial motor vehicles, finding compelling governmental safety interest and a reduced expectation of privacy by individuals who voluntarily chose to enter a highly regulated profession with periodic extensive examinations and urinalysis.

IBEW v. U.S. Nuclear Regulatory Commission[264]
The Ninth Circuit Court of Appeals affirmed that all employees at a nuclear power plant could be randomly tested, including clerical, warehouse and maintenance employees not engaged in safety-sensitive work and who did not have access to the plant's critical areas.

***American Federation of Government Employees, Local 1533 v. Cheney*[265]**
The Ninth Circuit Court of Appeals disapproved of blanket drug testing of employees with clerical positions, such as pathologists and dental hygienists. And, in *Luck v. Southern Pacific Transp. Co*.,[266] a California court found that a computer programmer was illegally fired for refusing to provide a urine sample as part of an unannounced drug test because the employee did not perform a safety-sensitive job and the employer had not shown a compelling interest in detecting drug usage by the particular employee.

As part of a judicial analysis of drug testing plans by courts throughout the country, a district court in Northern California, in *American Federation of Government Employees v. Derwinski*,[267] offered a specific constitutional analysis of issues such as randomness, reasonable suspicion, post-accident and follow-up testing. The court ruled that certain positions were not sufficiently safety- or security-sensitive as to justify random testing; that reasonable suspicion standards were overbroad as to non-safety/security-sensitive employees (in that factors were not limited to on-duty impaired work performance), and that "a pattern of abnormal conduct or erratic behavior" was too broad to support a conclusion of reasonable suspicion and did not comport with conduct consistent with drug use. The court also concluded that the post-accident testing guideline left too much discretion in the supervisor's hands, given that the supervisor must decide whether "the circumstances of the accident or unsafe act" justified testing. Finally, the follow-up testing component was deemed valid when random testing was monthly with a maximum of twelve tests during a one year period.

One California appellate court has held that the state constitutional right to privacy creates a public policy that may serve as the basis of a wrongful discharge claim arising from an employee's refusal to submit to random drug testing.[268] Another California appellate court has disagreed, stating that refusal to submit to drug testing implicates privacy rights, but not public policy.[269] Wrongful termination claims generally turn upon an analysis of whether the testing program is reasonable.

(See the Liebert Cassidy Whitmore workbook on "Issues and Challenges Regarding Drugs and Alcohol in the Workplace" for more information.)

In summary, if a public agency implements a random drug testing policy, it should limit testing to employees in positions which substantially affect the public safety and/or which provide access to truly sensitive information.

3. IMPLEMENTATION OF DRUG AND ALCOHOL TESTING PROGRAMS AND DUTY TO BARGAIN

a. Necessity of a Written Testing Policy

Employers who plan to use reasonable suspicion testing should develop a written policy which notifies employees that they may be subject to drug and/or alcohol testing if the employer has a reasonable suspicion that the employee is under the influence of illegal drugs and/or alcohol at work. The policy should also notify employees of the consequences of a failed drug test. A written policy, however, does not serve as a substitute for the requirement of reasonable suspicion. It instead serves to ensure that testing is implemented in a fair and reasonable manner.

Employers also should provide training to all supervisory and management employees responsible for determining whether reasonable suspicion exists to conduct the testing. The training should include recognition of the physical and behavioral characteristics of a person under the influence of drugs and/or alcohol.

> ***Kraslawsky v. Upper Deck Co,***[270]
> The employer informed its employee, Kraslawsky, that it would like to hire her as an executive secretary, conditioned upon her undergoing a medical examination and successfully completing a drug and alcohol test. Kraslawsky took the test and it revealed the presence of drugs which Krasklawsky claimed were prescription drugs. She obtained a doctor's note confirming her need for medication and she was hired.
>
> Before assuming the position, she signed a copy of the employee handbook that stated that the company "may require an employee to submit to monitored tests whenever it has reasonable cause to believe that an employee is under the influence of intoxicants…. An employee's refusal to consent when requested may result in disciplinary action." Eight months later, Kraslawsky was asked to drive to a medical facility and provide a urine sample for a drug test. She refused to take the test and was dismissed.
>
> The company argued that it had reasonable cause to test Kraslawsky because she signed the employee handbook and since she had appeared to be under the influence of intoxicants. Her supervisor claimed that her "speech was slurred, that her demeanor was lethargic, that her eye contact was not there." Kraslawsky refuted the supervisor's observations and stated that she answered all of the questions in her normal manner of speech and that the supervisor possessed no qualifications or training to determine whether someone was under the influence of intoxicants. Ultimately, the court held that there was a factual question as to whether the company had reasonable suspicion to test Kraslawsky for drugs and that it could not rely merely on its personnel rules as a basis for testing.

b. Duty to Bargain

Employers will almost always have a duty to bargain with the exclusive representative of their employees before implementing a drug or alcohol testing program since it affects the terms and conditions of employment. The duty of local agencies in California to bargain with representatives of their employees is governed by the Meyers-Milias-Brown Act (MMBA). Gov. Code § 3501, *et seq*. In *Holliday v. City of Modesto*, the court held that employee drug testing constituted a condition of employment, and was subject to negotiation with the union under the MMBA.[271]

In *Holliday*, the City of Modesto fire chief ordered a firefighter to submit to a drug test based on information that the firefighter possessed marijuana. While the Fire Department had a rule prohibiting the possession or use of illegal drugs or narcotics, the Department did not have a negotiated drug testing policy. Therefore, the court held that the fire chief's order that the firefighter submit to a drug test was unlawful and in violation of the MMBA.

In light of the *Holliday* case, local government employers are prohibited from testing employees for drugs and/or alcohol without a negotiated policy.

B. DOT-REGULATED DRUG AND ALCOHOL TESTING

Every employer in the United States who employs drivers of "commercial motor vehicles" or who operates a transit system in an urbanized area must be in compliance with the United States Department of Transportation regulations (implementing the Federal Omnibus Transportation Employee Testing Act of 1991). These regulations require that the employer adopt a drug and alcohol testing policy, in accordance with the regulations, for employees in "safety-sensitive functions," e.g., employees who drive vehicles with a gross vehicle weight of at least 26,001 pounds, or vehicles designed to transport 16 or more passengers, or vehicles which transport hazardous materials.

Most relevant to the privacy issues discussed in this workbook is the regulation that requires an employer to request particular drug and alcohol testing records that were made during the two years prior to the date that a new applicant or a current employee first requests transfer to a safety sensitive job.[272] The following is a summary of the requirements of this regulation.

1. RECORDS CHECK REQUIREMENT

The DOT regulation codified at Title 49 Code of Federal Regulations section 40.25 requires an employer to request particular drug and alcohol testing records that were made during the two years prior to the date of: 1) a new applicant's application for a safety-sensitive job; or 2) a request of a current employee to transfer to his or her first safety-sensitive job with that employer.[273] If the applicant or employee refuses to provide a written consent for this information, the employer cannot permit that person to perform safety-sensitive functions.[274]

2. THE INFORMATION TO BE RELEASED

The particular information that the employer must request is: 1) alcohol tests with a result of 0.04 or higher alcohol concentration; 2) verified positive drug tests; 3) refusals to be tested (including verified adulterated or substituted drug test results); 4) other violations of DOT agency drug and alcohol testing regulations; and 5) documentation of the employee's successful completion of DOT return-to-duty requirements (including follow-up tests). If the previous employer does not have information about the return-to-duty process (e.g., employer did not hire an employee who tested positive on a pre-employment test), the employer may obtain this information from the employee.[275] In addition, the information obtained from the previous employer also includes any drug or alcohol test information obtained from previous employers.[276]

3. WHEN THE INFORMATION MUST BE OBTAINED

The information must be obtained, "if feasible," before the employee first performs safety-sensitive functions. If that is not feasible, the employer must obtain the information as soon as possible. In any event, the employer must not permit the employee to perform safety-sensitive functions after 30 days from the date on which the employee first performed safety-sensitive functions, unless the employer has received the information or has made a good faith effort to obtain the information.[277]

4. CONSEQUENCES OF PRIOR VIOLATIONS

If the employer obtains information that the employee has violated a DOT agency drug and alcohol regulation, the employer must not allow the employee to perform safety-sensitive functions unless the information indicates that the employee has subsequently complied with the DOT return-to-duty requirements.[278]

5. DUTIES OF REQUESTING AND RECEIVING EMPLOYERS

The requesting employer has the duty to provide the prior employer with the employee's written consent to release the information.[279] The employer who receives a written consent must review it and then "immediately release the requested information" to the employer making the inquiry.[280] The information may only be released in a manner that ensures confidentiality.[281]

6. RECORD-KEEPING

An employer who releases information must maintain a written record of the information released, including the date, the party to whom it was released, and a summary of the information provided.[282] The employer requesting the information must maintain a written, confidential record of the information obtained or of its good faith efforts to obtain the information.[283] The employer must retain these records for three years from the date of the employee first performed safety-sensitive duties for that employer.[284]

Request Information Directly From the Employee or Applicant. Finally, Section 40.25 requires the employer to also ask the applicant or employee whether he or she has tested positive, or has refused to test, on any pre-employment drug or alcohol test for any safety-sensitive job applied for but not obtained during the prior two years.[285] If the individual admits that he or she has had a positive test or has refused to submit to testing, the employer must not use the individual to perform safety-sensitive functions until the individual documents successful completion of the return-to-duty process.[286]

C. MAINTAINING DRUG AND ALCOHOL TEST RESULTS

For purposes of complying with privacy laws, employers should treat drug and alcohol test results and information with the same care as with the results of medical examinations. This includes strictly maintaining the confidentiality of the drug and test results and storing them in a secure place that is separate from regular personnel records. An employer has an affirmative duty to prevent disclosure of such information without the employee's consent and therefore must establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information. For a detailed discussion of these requirements, refer to the section in this workbook pertaining to maintenance of medical information.

SECTION 5 PERSONNEL RECORDS AND FILES

Legal snapshot: Personnel Records and Files	
Applicable laws:	• Constitutional Right of Privacy (Cal. Const. art. I, § 1) • The Ralph M. Brown Act ("Brown Act"), Gov. Code §§ 54950 *et seq*. • California Public Records Act, Gov. Code §§ 6250 *et seq* • Public Safety Officers' Procedural Bill of Rights Act, Cal. Gov. Code §§ 3300 *et seq.* • Various other California statutes • Common law torts
Who and what is protected?:	• All current and past employees • Most personnel records and files

Generally, employers must NOT:	• Make or permit disclosures of personnel information or files absent written employee authorization or court order[287] • Make authorized or ordered disclosures that are broader than authorization or order[288] • Waive the privacy rights of employees[289]
Applicable balancing test:	• Employee's interest in confidentiality of personnel records *v.* the employer's or public interest in disclosing them

A. INTERNAL ACCESS TO PERSONNEL RECORDS AND FILES

1. AN EMPLOYEE'S RIGHT TO RESPOND TO INFORMATION IN HER OR HIS PERSONNEL FILE

California Education Code section 87031 requires that a district give its employees notice and the opportunity to review and comment on any derogatory information before placing that information in the employees' personnel files.

In *Miller v. Chico Unified School District, Board of Education*,[290] the California Supreme Court held that the Board's failure to place 20 confidential memoranda criticizing Miller's conduct in Miller's personnel file, prior to reviewing and considering the memoranda in its decision to reassign Miller, violated Miller's right to receive notice and the opportunity to comment on the information. Miller asserted that if the Board had given him the opportunity to comment upon the material at the time the Board compiled it, he could have easily contradicted or explained the information. The court rejected the Board's assertion that the statute did not apply because the Board never placed any of the memoranda in Miller's personnel file. The Court made clear that the Board could not avoid the statute's requirements by maintaining a "personnel file" for certain documents relating to an employee, while segregating elsewhere under a different label, materials that might serve as a basis for affecting the status of the employee's employment. The Court held that unless a school district gives an employee reasonable notice of the derogatory information, so that the employee can gather pertinent information in his/her defense, the school district cannot use the information in reaching any decision affecting the employee's employment status.

In *Woodland Joint Unified School District v. Commission of Professional Competence*[291], the California Court of Appeal held that Education Code Section 44031 does not require that a school district warn a teacher about his or her offensive conduct before the school district may dismiss the teacher for "evident unfitness for service." Although Education Code section 44031 requires that a school district disclose derogatory written material to a teacher, unless the school district reduces the conduct to writing, the Education Code does not require that the school district warn the teacher about the offensive conduct.

2. PRIVACY RIGHTS OF THIRD PARTIES WHEN EMPLOYEES INSPECT OWN PERSONNEL FILES

California Labor Code section 1198.5 gives all employees (except public safety officers whose inspection right derives from the POBR and firefighters whose inspection rights are found in the Firefighters Procedural Bill of Rights Act ("FBOR")) the right to inspect their own personnel files. Education Code section 87031 expressly applies the right of inspection under California Labor Code section 1198.5 to employees of community college districts. This right extends to all documents which the employer maintains relating to the employee's performance or to any grievance concerning the employee.

Under Government Code section 3305, public safety officers are entitled to inspect any adverse comment before it is entered into their personnel file. The term "adverse comment" includes citizen complaints.[292]

- Investigation of a possible criminal offense
- Letters of reference
- Ratings, reports, or records obtained prior to the employee's employment
- Ratings, reports or records prepared by an identifiable examination committee
- Ratings, reports or records obtained in connection with a promotional examination

California Courts have also recognized the right of privacy in third parties who prepare ratings, reports, and records that is contained in Article I, Section 1 of the California Constitution.[293] This Constitutional right of privacy in third parties also extends to public safety officer personnel file inspections. Their inspection rights do not apply to unfavorable comments recorded by interviewers in connection with a promotional examination.[294]

***Board of Trustees v. Superior Court*[295]**
An employee sought discovery of the entire contents of his own personnel file. The University refused to produce written references and statements made by third parties under a guarantee of confidentiality. The Court of Appeal held that the University should make appropriate deletions and produce all documents which could be produced without divulging the identity of the third parties who had been guaranteed confidentiality.

***Brutsch v. City of Los Angeles*[296]**
The Court of Appeal refused to permit police officers access to interviewers' rating sheets which contained the interviewers' comments recorded during the oral interview portion of a promotional examination. The Court recognized the City's legitimate interest in protecting the privacy of the interviewers whom had been assured that their comments would be confidential and rejected plaintiff's suggestion that the City redact the names of the interviewers from the rating sheets to allow disclosure. The Court held that plaintiff's proposed solution was inadequate for three reasons: (1) since the comments are in the interviewers' own handwriting, plaintiffs may recognize the writing; (2) the possibility that the wording of some of the comments would in and of itself provide a clue to the drafter's identity; and lastly, (3) some interviewers made their comments on the examination forms themselves presumably in reliance on the promised confidentiality.[297]

Furthermore, the California Supreme Court has held that Government Code section 3303, subdivision (f), of the Public Safety Officers Procedural Bill of Rights Act does not grant a peace officer, subject to an internal affairs investigation, a right to investigative reports and complaints prior to being interrogated.[298]

3. CHECKLIST: EMPLOYEE PERSONNEL FILE INSPECTION PROCEDURE

Employers may want to consider the following checklist in implementing an employee personnel file inspection procedure:

- ❑ Require the employee to provide a written request for access to the file.
- ❑ Review the file to determine whether any of the statutory exemptions apply (e.g., letters of reference regarding county employee, criminal investigations). If so, remove such documents from the file.
- ❑ Determine whether any of the documents in the file are from individuals who have been given an assurance of confidentiality. If so, remove these documents from the file.
- ❑ Enter a notation indicating date and time of employee's inspection.

Some states expressly require employees to submit a written form requesting access to their personnel files. The purpose of such a requirement is to identify the requesting individual and to

avoid disclosure to ineligible individuals. Even though California does not expressly provide for this requirement, employers should maintain records of requests to inspect personnel files together with detailed information concerning the inspection. For example, the records custodian should record the time the inspection occurred and identify which documents were reviewed and copied. The custodian may also wish to obtain from the requesting employee a signed statement that the inspection occurred. Detailed records concerning the inspection of personnel files will provide evidence of an employer's compliance with the access statutes.

4. CONTROLLING INTERNAL ACCESS TO PERSONNEL FILES

Employers have a duty to see that information contained in an employee's personnel file or supervisor's desk folder is not disclosed to others in the agency in ways that are unfair to the employee. For example:

- Personnel and payroll records should only be available internally to authorized users on a need-to-know basis.
- Security records or records relating to security investigations should be maintained apart from other records, but access need not be given to the employees unless the information is incorporated into their personnel files or is used for discipline, termination, promotion or evaluation.
- Medical records used for work restrictions and life and health insurance records should be kept confidential. These records should not be made available for use in any employment decision.
- Records of work-related insurance compensation, disability, sick pay should be available internally only to authorized recipients on a need-to-know basis.

B. THIRD PARTY ACCESS TO PERSONNEL ACTIONS, RECORDS, AND FILES

1. BROWN ACT

The Ralph M. Brown Act (Brown Act), Government Code section 54950 *et seq.*, (significantly amended in 1994 – see the Liebert Cassidy Whitmore workbook on "The Brown Act" for current law) requires public agency governing boards and commissions to meet in public to take official action, unless an exception exists. One such exception exists in Government Code section 54957. This section allows public agencies, including community college districts, to meet in closed session to consider the appointment, employment, evaluation of performance, or dismissal of a public employee. The Brown Act also provides that any employment action taken in closed session must be publicly reported at the public meeting during which the closed session takes place or at the next public meeting,[299] though there are some technical exceptions to this provision.

With regard to privacy rights of those attending meetings, Section 54953.3 provides that a public agency cannot force a speaker participating in a public meeting to state his or her name and address for the record. Agencies may only ask participants to volunteer that information. Additionally, agencies cannot compel speakers at public meetings to provide "personally identifiable information."

a. Closed Session for Certain Personnel Matters

A closed session may be held during a regular or special meeting to consider the appointment, employment, evaluation of performance, or dismissal of a public employee or to hear complaints or charges brought against an employee by another person or employee unless the employee requests a public hearing.[300]

Under the Brown Act, an "employee" includes an officer or an independent contractor who functions as an officer or an employee but excludes any elected official, member of a legislative body, or other independent contractors. Thus, the governing body may not meet in closed session regarding the filling of a vacancy on the governing board. It may not meet in closed session to discuss entering into a contract even if that contract would provide for personal services.

Under Government Code section 54957, prior to holding a closed session on specific complaints or charges against an employee, the agency must give the employee written notice of his or her right to have the complaints heard in open rather than closed session. The notice is required to be delivered personally or by mail at least 24 hours prior to the session. Closed sessions held under section 54957 may not include discussion or action on proposed compensation, except for a reduction in compensation resulting from discipline. Section 54957 permits discussion of personnel actions in a closed session to protect the affected employee's privacy rights. The California Attorney General has stated that the "purpose in permitting an executive session concerning personnel matters is to avoid undue publicity and embarrassment to the affected employee."[301]

The following are decisions which describe the circumstances under which an agency may or may not hold a closed session under section 54957:

> ***Kolter v. Com. of Professional Competence of the Los Angeles Unified School District[302]***
> The governing board of the Los Angeles Unified School District met in closed session and initiated the process to dismiss Kolter, a permanent certificated elementary school teacher. Kolter did not receive any pre-meeting notice of the session or the charges against her. After the closed session, the District notified Kolter of its intent to dismiss her from her employment. The Court of Appeal held that the board was not required to give Kolter 24 hour notice of the meeting because it did not conduct an evidentiary hearing on the charges against her. Rather, it considered whether those charges justified the initiation of dismissal proceedings which would later result in an evidentiary hearing.
> The *Kolter* court found that the Legislature used the verb "hear" in connection with "complaints or charges," but the verb "consider" in connection with

"dismissal of a public employee."[303] The word choice is significant. To "consider" is to deliberate upon, while to "hear" is to listen to in an official capacity. A "hearing" is a formal, official proceeding, usually open to the public, with definite issues of fact or of law to be tried, in which witnesses are heard and evidence presented.[304]

LCW Practice Advisor

The *Kolter* case holds that 24 hours notice is not required before the legislative body decides to initiate discipline against an employee. A cautious and conservative approach is to continue to provide 24 hours notice until the exact boundaries of the *Kolter* decision are litigated in the coming years.

The *Kolter* decision turned on the fact that the board's action in closed session was not the final decision. If your legislative body's consideration of discipline is the agency's final decision, 24 hours notice is still required.

Furtado v. Sierra Community College

The California Court of Appeal held that negative performance evaluations do not constitute "complaints or charges" against an employee pursuant to Government Code § 54957 of the Brown Act.[305] Arguably then, a public employer may consider in closed session whether to retain an employee based on evaluations despite the employee's request to respond in open session. However, be careful in light of certain Court of Appeal decisions, e.g. *Morrison v. HACLA, infra* and *Moreno v. City of King City, infra*.

Fischer v. Los Angeles Unified School District

The California Court of Appeal held that the evaluation of the performance of probationary teachers does not constitute the bringing of "specific complaints or charges," and, therefore, the teachers are not entitled to notice nor have the right to request an open session of the school board meeting in which the decision to re-elect or not re-elect the teachers will be made.[306]

Bollinger v. San Diego Civil Service Commission

A civil service commission's closed session hearing to discuss appropriate discipline for employee misconduct (including possible demotion) did not violate the employee's Brown Act right to an open, public hearing.[307] **Be Cautious!**

Morrison v. Housing Authority of the City of Los Angeles Board of Commissioners

The Court of Appeal ruled that a board considering the recommendation of an arbitrator violated Government Code section 54957 by not providing the employee with 24-hours notice of his or her right to have the complaints or charges heard in open session before the board reviewed the arbitration record supporting the arbitrator's recommendation,[308] especially where the Board rejected the arbitrator's recommendation and, instead, imposed termination.

b. Notice and Reporting of Closed Session Personnel Matters

Government Code section 54957.7 is similarly instructive. This section requires the legislative body of a local agency to state the reasons and authority for holding a closed session at the open session during which the closed session took place or at the next public session held by the agency. This section further provides: "Nothing in this section shall require or authorize the giving of names or other information which would constitute an invasion of privacy or otherwise unnecessarily divulge the particular facts concerning the closed session."

In order to comply with the public announcement requirements and at the same time respect an employee's privacy rights, employee numbers, and not names, should be used when reporting personnel decisions made in closed session. This would assure an employee's anonymity and enable an employer to comply with the Brown Act. Please note, however, that employee social security numbers must not be used in announcing the action.

City's Overly-Cautious Notice of Personnel Matter Resulted in Insufficient Notice and City's Termination of an Employee Deemed Null and Void[309]

In October 2002, the City of King City Council held a special meeting. On the agenda for the meeting was a single item: "Per Government Code Section 54957 Public Employee (employment contract)." The minutes from this meeting stated that there was "no reportable action taken in closed session." Several days following the meeting, Keith Breskin, the City Manager, gave Roberto Moreno, the finance director, a two-page memorandum that informed Moreno he was being terminated and detailed five alleged incidents of Moreno's misconduct. Moreno was given no opportunity to respond to the accusations before his termination became effective.

Moreno filed a petition for a writ of mandate alleging that the City had violated the Brown Act in terminating his employment and sought to have his termination declared null and void. Following an evidentiary hearing, the trial court granted Moreno's petition. In addition to declaring that Moreno's termination be declared null and void, the court awarded Moreno damages, fees, and costs. The Court of Appeal affirmed. Among other bases for its holding, the Court ruled the City's October 17 agenda was in violation of the Brown Act because it did not provide a brief general description of the business to be transacted or discussed at the meeting. The City argued that a more general

description of the business on the agenda - i.e., "Moreno's dismissal" – may have violated Moreno's privacy rights. In response, the Court stated that the City could still properly specify the action while protecting Moreno's privacy rights. The Court suggested that if the agenda stated "Public Employee Dismissal," this would have been a sufficient description under the Brown Act.

c. Pending Litigation Concerning Personnel

According to an opinion issued by the California Attorney General, a local agency's legislative body, such as a city council or school board, may rely upon the "pending litigation" exception of the Brown Act to go into closed session to deliberate and act upon settlement of a lawsuit. This interpretation of Government Code section 54956.9 expands the right of legislative bodies to confer regarding pending litigation with its attorney in closed session.[310]

Appointment of Employees/Nomination of Candidates

In *Gillespie v. San Francisco Public Library Commission,* the California Court of Appeal held that the Brown Act's exception to open meetings for appointment of employees encompasses nomination of candidates by committees that lack the power to appoint.[311]

The San Francisco Public Library Commission held a closed session to consider the appointment of an Acting City Librarian, and subsequently submitted three names to the Mayor for consideration. After the Mayor appointed one of the candidates, the Commission stated that it would not disclose the names of the two unsuccessful candidates. Public Access Project filed a petition for writ of mandate to set aside the Library Commission's nominations, claiming that the Commission violated the Brown Act by meeting in closed session and failing to publicly announce the nominations at that meeting. The court denied the petition. Public Access Project appealed.

The Court of Appeal affirmed. The court held that the fact that the Commission did not have the power to appoint the Acting City Librarian did not prevent the Commission from meeting in closed session. Under the San Francisco City Charter, the Mayor shares the power of appointment with the Library Commission. The Court concluded that the Commission can nominate Department head candidates in closed session because such meetings are consistent with the purposes of Government Code section 54957, i.e., "to foster candid discussions by members of the legislative body concerning the qualifications of staff or prospective staff members without subjecting the latter to public embarrassment." Moreover, the court held that the Brown Act makes clear that only the actual appointment, and not merely nomination, must be reported on the day of the nomination.

2. CALIFORNIA PUBLIC RECORDS ACT

The California Public Records Act, Government Code section 6250 et seq., also requires employers to exercise caution in areas implicating employee privacy rights. Non-profit organizations of local government agencies and officials that are supported solely by public funds are now encompassed within the Act's parameters.

The California Public Records Act[312] was enacted with the objective of increasing public access to government records. Like the federal Freedom of Information Act[313] upon which it was modeled, the general policy of the Act favors disclosure.[314] Support for refusal to disclose information "must be found, if at all, among the specific exceptions to the general policy that are enumerated in the Act."[315]

The Act applies to "public records," which are defined 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."[316] The mere custody of a writing by a public agency does not make it a public record, but if a record is kept by an officer because it is necessary or convenient to the discharge of his official duty it is a public record.[317]

In *City of San Jose v. Superior Court*[318], a California Court of Appeal made a distinction between *messages stored on personal electronic devices and personal accounts, and messages stored on* electronic devices issued by the agency. The court held that CPRA does not impose on an agency an affirmative duty "to produce messages stored on personal electronic devices and accounts that are inaccessible to the agency, or to search those devices and accounts of its employees and officials upon a CPRA request for messages relating to City business."[319] The California Supreme Court has granted review of the Court of Appeal's decision[320] and, while the California Supreme Court's decision is pending, the Court of Appeal's decision may not be cited as precedent or relied upon by anyone.

Section 6254 provides exemptions to the disclosure requirements of the Act for certain records. The exemptions are designed to protect privacy interests of individuals whose data or documents come into governmental possession.[321] California courts have construed the statutory exemptions narrowly in order to accomplish the general policy of disclosure.[322] Importantly, Section 6254(c) exempts **personnel, medical** or similar files if the disclosure would "constitute an unwarranted invasion of personal privacy." Courts will employ a balancing test in determining whether records should be exempt from disclosure under Section 6254(c) and weigh the individual's right to privacy against the right of the public to oversee the actions of governmental employees.[323]

a. Home Addresses and Telephone Numbers

Section 6254.3 excludes the home addresses and home telephone numbers of state employees and employees of school districts and county offices of education from the definition of "public record" and exempts them from public inspection, except in specifically delineated situations.

Telephone numbers relating to calls made and received by city council members have been found exempt from the disclosure requirements of the Public Records Act, based upon the deliberative process privilege. In reaching this conclusion, the court analogized the facts of the case to a California Supreme Court case that ruled that releasing copies of a state Governor's appointment calendars and schedules for a five-year period would compromise the deliberative process. The deliberative process privilege protects from disclosure the substance or direction of judgment and mental processes.[324]

b. Employment Contracts

Section 6254.8 also provides that employment contracts between a public employer and a public official/employee are public records and are not exempt from disclosure. However, the California Court of Appeal clarified that documents referenced in but not made a part of the contract and not otherwise required to be disclosed are not subject to public disclosure.[325]

***Braun v. City of Taft*[326]**

The court held that two letters in an employee's personnel file which appointed that employee to a certain position and then rescinded it were public records since the letters constituted an employment contract. The Court also noted that salary information was public information and suggested that home addresses and phone numbers, birth date, social security and credit union numbers, although personal, were not in any way embarrassing. The implication was that the public may be entitled to such information. The Court in *Braun* also stated that Section 6524(c) cannot be interpreted as exempting an entire file from disclosure where only a portion of the file contains documents whose disclosure would constitute an unwarranted invasion of privacy. Moreover, the fact that a public record may contain some confidential information does not justify withholding the entire document.

Versaci v. Superior Court

The court held that documents referenced in but not made a part of the contract are not subject to public disclosure.[327] Dr. Sherrill Amador was hired by the Palomar Community College District to be its Superintendent and President under a four-year contract. One paragraph in the contract stated that Dr. Amador would receive an annual written evaluation that would be based on her overall performance and "mutually agreed upon goals and objectives established each year." On an annual basis, in closed session, Dr. Amador and the board mutually established her personal performance goals for the academic year.

Prior to the expiration of Dr. Amador's contract, the Board voted to extend her contract and to increase her compensation. Concerned about salary increases of administrators, Rocco Versaci, the president of the District's faculty union, submitted a request under the Public Records Act for a copy of Dr. Amador's annual performance goals. The District denied the request. The District asserted that the Act did not require disclosure of the goals and, further, disclosure would violate Dr. Amador's right to privacy. Versaci petitioned for a writ of mandate ordering the District to disclose the goals.

The lower court denied Versaci's petition, and the appellate court affirmed. Government Code section 6254.8 provides that every employment contract between a state or local agency and a public employee is a public record. However, mere mention of an external document (the goals) in the employment contract does not automatically render the external document part of the contract and subject to disclosure. An external document will not be part of the contract unless there is "clear and unequivocal" language in the contract that the parties intended the external document be made part of the contract.

In addition, Dr. Amador's personal performance goals were part of her annual performance evaluation. Because Dr. Amador had a reasonable expectation of privacy in her performance evaluation, she also had a reasonable expectation of privacy in her personal performance goals.

c. *Employee Salaries*

Salaries of public employees by classification or without identifiable names have long been open for public inspection. There had been a significant amount of litigation regarding the disclosures of specific salaries along with employee names, but the controversy has been laid to rest, at least in California by the California Supreme Court's decision in *International Federation of Professional and Technical Engineers v. Superior Court.* In this case the Court held that information regarding a specific public employee's salary is discoverable under the Public Records Act. As the Court explained "in light of the strong public policy supporting transparency in government, an individual's expectation of privacy in a salary earned in public employment is significantly less than the privacy expectation regarding income earned in the private sector."[328]

Finally, note that personal information such as date of birth, address, phone number, and social security number, which may also be contained in a salary card are not a matter of public record. Therefore, employers should be advised that where non-exempt materials are not inextricably intertwined with exempt material, employers must make reasonable efforts to segregate those materials. This segregation will serve the objective of the Public Records Act by making those public records available for public inspection.

d. Complaints against Employees

Government Code section 6254 of the Public Records Act further provides that in making a report available to the public of certain crimes, including rape, the address of the victim shall not be disclosed and the name of the victim may be withheld at the victim's request or at the request of the victim's parents if the victim is a minor. This section was amended in 1991 to provide that the above applies to victims of certain crimes committed because of the victim's race, color, religion, nationality, country of origin, ancestry, disability or sexual orientation.

Government Code section 6254, subdivisions (f)(1) and (2) of the Public Records Act has been found to be limited to contemporaneous disclosure of individualized arrest information. The Act does not require release of records showing arrests by a law enforcement officer over a ten-year period.[329]

In *Marken v. Santa Monica Unified School District*,[330] the Court of Appeal held that disclosure of a school district's investigation of allegations that teacher sexually harassed student was warranted under California public records act because public interest in knowing how the school district handled such matters outweighed the teacher's privacy rights. The Court stated that a complaint of misconduct which is upheld by the agency or results in discipline must be disclosed. If the complaint is not sustained, it is still subject to disclosure if it is of substantial nature and there is reasonable cause to believe the complaint is well founded. Although the teacher did not occupy a high profile position, that factor is only relevant to determine when accusations of misconduct should be disclosed even if not well founded. The Court ordered the district to disclose the investigation report and the reprimand with the names and personal information of the student and the witnesses redacted.

Prior cases involving California Public Records Act requests for personnel records involved more extreme cases where the complaint involved violence and sexual abuse, or a high profile public official. [331] But this case clarifies that if a charge of misconduct results in employee discipline, even minor discipline, the complaint must be disclosed upon request.

In certain circumstances, the Court may require the release of the report, even if accused is exonerated for the most part of the allegations, because the investigation is of a high ranking official. In *BRV v. Superior Court*[332], although the district superintendent was exonerated of all serious allegations except for those relating to outbursts of anger, the court found that the public's interest in knowing why the superintendent was exonerated and how the district conducted the investigation outweighed any privacy interests that the superintendent had in the report, although some redactions were permitted to protect the privacy interests of witnesses. Similarly in *Caldecott v. Superior Court*[333], the court order disclosure of the district's response to a hostile work environment complaint by the Executive Director of Human Resources against the district's superintendent. While the district did not impose discipline and the allegations were not sustained, the complaint involved allegations of wrongdoing against a high ranking public official complaint. The court was unable to conclude that the allegations were so unreliable that they could be anything but false and there was a strong public interest in knowing how the district's board treated serious allegations of misconduct against a high ranking public official.

The court in *Caldecott* also permitted redactions to protect the privacy rights of third party individuals.

However, the Court of Appeal found in *Petaluma v. Superior Court of Sonoma County*[334] that investigation materials were protected by the attorney-client privilege where an attorney investigator conducted the investigation even though the investigator's role was limited to a factual investigation and did not provide legal advice. The case involved a discovery dispute and was not the California Public Records Act. However, it is likely that the same analysis would apply to allow a public agency to rely on the attorney-client privilege and the attorney work product doctrine in refusing to disclose an attorney prepared investigation report.

Public agencies must carefully evaluate any requests for investigation and disciplinary documents. With the exception of police officer personnel records which are subject to some additional protection under the law, a public agency may be required to release such documents. The California Supreme Court has limited access to records of police investigations except for certain information about crimes and arrests. The court rejected news media arguments that the state public records law must follow federal (Freedom of Information Act) disclosure standards. Under federal standards, an investigative record must be released unless it would interfere with enforcement or a fair trial, violate privacy, identify a confidential informant or endanger someone's life.

In *City of Hemet v. Superior Court*,[335] the court held that a police department internal investigation report relating to allegations of police misconduct was protected from disclosure under the Public Records Act as records the disclosure of which was exempted or prohibited by the confidentiality provisions of Penal Code section 832.7.

Finally, the Public Records Act mandates that a party who prevails in a lawsuit pursuant to the Act is entitled to attorneys' fees.[336] Consequently, public agencies should consider seeking consent for disclosure of possibly confidential records prior to refusing such Public Records Act requests.

e. *Peace Office Administrative Appeal from Discipline*

The California Supreme Court determined that records relating to a peace officer's administrative appeal from discipline were exempt from disclosure under the Public Records Act. In *Copley Press, Inc. v. Superior Court*, a San Diego newspaper's publisher sought to obtain information regarding a deputy sheriff's administrative appeal of his termination. The County of San Diego and San Diego Civil Service Commission refused to make full disclosure of the records, and the California Supreme Court ultimately upheld their decision. The Court observed that Government Code Section 6254(k) of the CPRA protected "[r]ecords, the disclosure of which is exempted or prohibited pursuant to federal or state law . . . ." One such state law, the Court observed, is California Penal Code section 832.7(a), which provides that certain "[p]eace officer or custodial officer" records and "information obtained from these records [ ] are confidential and shall not be disclosed in any criminal or civil proceeding except by discovery pursuant to Sections 1043 and 1046 of the Evidence Code." The statute applies to "personnel records," which California Penal Code section 832.8 defines as "any file maintained

under [an officer's] name by his or her employing agency and containing records relating to," among other things, "[p]ersonal data" and "[e]mployee advancement, appraisal, or discipline."

The publisher argued that by its terms Section 832.7's protection applied only to requests made in civil and criminal proceedings. The Supreme Court rejected the argument, reasoning that the statutory framework did not support the anomalous result that the public could freely request discipline records under the Public Records Act, whereas civil and criminal litigants faced substantial hurdles in obtaining disclosure. The publisher argued next that because the civil service commission that considered the peace officer's disciplinary appeal was not technically his "employer," Section 832.7's protections would not apply. The Court rejected that argument as well, reasoning that the protections of Section 832.7 should not turn on the happenstance of whether the appeal system was structured so that a civil service commission rather than an employing agency heard an employee's administrative appeal. Finally, the newspaper made generalized arguments for access based on the common law and constitutional principles, which the Court rejected.[337]

Technically, *Copley* applies only to requests for administrative appeal materials for peace officers, because the case rests on the Public Records Act, Section 6254's incorporation of specific laws applicable to peace officer records, such as California Penal Code section 832.7. But Copley's general reasoning and approach should help with protection of the discipline records for other types of public employees as well, particularly if the employer can locate specific laws restricting disclosure of the type of information in question.

f. Disclose the Names of Peace Officers Involved In a Critical Incident Unless a Particularized Showing of Threat of Harm Has Been Made

In *Long Beach Police Officers Assn. v. City of Long Beach*[338], the California Supreme Court reviewed whether police departments are required to disclose the names of officers involved in shooting incidents while on duty in response to a Public Records Act request. The Court declined to adopt a blanket rule that required or denied the disclosure of the names. Instead, the Court required an assessment based upon the particular facts of each case to determine whether a sufficient particularized showing of threat of harm had been made by the department to prevent disclosure of the names. In that particular case, *Long Beach Police Officers Assn. v, City of Long Beach*, the Court found that the required showing had not been made and that the names would need to be disclosed.

g. Report Prepared following Officer-Involved Shooting Is Subject to Disclosure Once Peace Officer Personnel Information is Redacted

In Pasadena Police Officers Association v. Superior Court339, a California court of appeals court determined that the Pasadena Police Department had redacted too much information before producing a report prepared by an independent consultant in response to a Public Records Act request. The report evaluated the Pasadena Police Department's investigation of the shooting of an unarmed teenager by two police officers, the adequacy of the department's training, and also recommended any needed institutional reforms. The report contained information from a criminal investigation as well as an administrative investigation. The court ordered that

information related to employee appraisal (e.g., officers' personnel information and officers statements made in the course of the department's administrative investigation) were confidential and must be redacted. However, portions of the report unrelated to employee appraisal (e.g., the department's criminal investigation) were not confidential and should not have been redacted.

h. Release to DA of List of Officers against Whom Findings of Dishonesty, Moral Turpitude or Bias Have been Sustained

The California Attorney General has opined[340] that Penal Code section 832.7(a) does not authorize a district attorney, for the purpose of complying with *Brady*, to directly review the personnel files of peace officers who will or are expected to be prosecution witnesses to determine whether any *Brady* issues apply. However, to "facilitate compliance with *Brady*," the CHP may lawfully release to the district attorney's office the names of officers against whom findings of "dishonesty, moral turpitude, or bias have been sustained, along with the date of the earliest such conduct." The district attorney may then use this information to comply with *Brady* requirements.

The California Attorney General, in issuing its opinion, relied on *People v. Superior Court (Johnson).*[341] In *Johnson*, the California Supreme Court determined that prosecutors do not have unfettered access to the confidential personnel records of police officers who are potential witnesses in a criminal case but must follow the same procedures that apply to criminal defendants in order to obtain information in those records (i.e., filing a *Pitchess* motion). Thus, the prosecutor may fulfill his or her *Brady* obligation if he/she informs the defendant that the department has informed the prosecutor that the personnel records of the officer may contain Brady information, and that the officers were important witnesses.

> ***Note:*** *Brady[342] requires the prosecution to disclose to the defense any exculpatory evidence, including potential impeaching evidence. This duty extends to others acting on the prosecution's behalf, including the police. The criminal defendant may then, under Pitchess[343], compel discovery of evidence in the law enforcement officer's personnel file that is relevant to the defendant's ability to defend against the criminal charge.*

i. No 60-Day Limitation in Public Records Act for Accessing Police Calls for Service Records

In *Fredericks v. Superior Court of San Diego County*[344], a Public Records Act request was made for all "complaints and/or request for assistance" relating to any burglary and identity theft in San Diego for the preceding six-month period. The request would require the department to redact a large number of Calls for Service reports, at a substantial cost of lost time in work days to complete the response to the request. In response, the City sought to limit the request to a 60-day time period and to recover more than its direct costs of duplication. The appellate court found that a 60-day limitation could not be read into the act for production of the reports. However, the court could apply a balancing test for the production of the requested information that could take into account the expense, inconvenience and work load burden of segregating

exempt from non-exempt information and redacting documents. The court could also set a time limitation if the balancing of the public interest factors supported one. The case was then remanded for the trial court to determine whether greater disclosures were warranted and to condition, if appropriate, any additional disclosures upon an additional imposition of fees and costs over the direct costs of duplication.

j. Inability to Prevent Newspaper from Publishing or Printing Confidential Peace Officer Personnel Information that May Have Been Illegally Obtained

In Association for Los Angeles Deputy Sheriffs v. Los Angeles Times Communications LLC 345, a California court of appeal held a police union could not prevent the Los Angeles Times from publishing or printing confidential peace officer personnel information that may have been illegally obtained. The court determined that no admissible evidence had been presented that the Times stole the information and a long line of federal and California cases protected the press under the First Amendment when it may have published or disclosed illegally-obtained content. The court further found that an injunction preventing the disclosing of the information was an unconstitutional prior restraint and that any privacy right processed by the deputies in their employment application information belonged to them and could not be asserted by their union.

3. UNION ACCESS TO PERSONNEL FILE AND CONTACT INFORMATION

A union is generally entitled to see an employee's personnel file if the employee consents to the disclosure. If the employee does not consent to the disclosure, a balancing test is applied. In *Detroit Edison Co. v. NLRB*,[346] the United States Supreme Court held that an employer did not commit an unfair labor practice by refusing to disclose, without a written consent from individual employees, aptitude test scores linked with employees' names in light of the sensitive nature of the testing information. The court stated:

> *A union's bare assertion that it needs information to process a grievance does not automatically oblige the employer to supply all the information in the manner requested. The duty to supply information under Section 8(a)(5) [of the NLRA] turns upon the circumstances of the particular case, and much the same may be said for the type of disclosure that will satisfy the duty. 440 U.S. at 314-15, 99 S.Ct. at 1131 (citations omitted).*

Thus, a balancing is required between the union's need to have information so that it can effectively carry out its functions as bargaining representative of the employees and the employee's legitimate right to privacy and the employer's interest in maintaining the confidentiality of his or her personnel file. The relevancy of the information sought by the union, the employee's privacy interest in the information sought and the safeguards provided to he employer to protect that privacy interest are the principal elements to be considered.[347]

Regarding employee home addresses, the California Supreme Court determined in *County of Los Angeles v. Los Angeles County Employee Relations Commission* that a public employer must disclose home contact information for all bargaining unit members (even non-union members) to the representatives for the bargaining unit.[348] It held that the failure to provide relevant information about non-member employees violated the County's obligation under the Meyers-Milias-Brown Act (MMBA) to bargain in good faith. The Court noted that the parties could negotiate or the Commission could adopt specific procedures to allow non-members to opt-out of providing their home contact information.

A public entity is required to disclose the work locations of various members even if the work location reveals that the member was under disciplinary and/or criminal investigation. In the PERB Decision *Los Angeles Unified School District*[349], the district temporarily assigned employees under disciplinary and/or criminal investigation to one of its Educational Service Centers ("ESCs"). The union demanded to bargain the working conditions of the ESCs and as part of the bargaining over this, asked the district to identify all unit members who were temporarily assigned to either an ESC or their home while under investigation, and the specific ESC to which they were assigned. The district provided the information but only after it gave the employees the opportunity to opt-out of the disclosure. Fifteenof the 276 employees opted - out of the disclosure. The union filed an unfair practice charge for not receiving all of the information requested. The ALJ decided that the unit members did not have a substantial privacy interest against the union's right to the information, and also that the district did not bargain the opt-out procedure in good faith before it implemented it. PERB affirmed, determining that the privacy interest of the members was minimal against the union's need for the information, and that the request was tailored to accommodate any privacy concerns (not asking for personnel files or investigation reports and offered to keep confidential the contact information).

An employer has no affirmative obligation to provide a union information about a pending disciplinary action about a represented employee without a request and without the employee's consent.[350]

4. WORKSITE INSPECTIONS OF PERSONNEL FILES BY IMMIGRATION ENFORCEMENT AGENTS

Effective January 1, 2018, the California Immigrant Worker Protection Act (AB 450) provides that, "except as otherwise required by federal law," an employer, or a person acting on behalf of the employer, shall not provide "voluntary consent" for an immigrant enforcement agent to:

- Enter non-public areas of the worksite, unless the immigration enforcement agent provides a judicial warrant[351]
- Access, review, or obtain employee records without a subpoena or court order.[352]

An employer will be subject to penalties for violating each of these provisions. The penalties are civil penalty of two thousand dollars up to five thousand dollars for a first violation, and five thousand dollars up to ten thousand dollars for each subsequent violation.[353] A violation is "each incident" where it is found that a violation occurred "without reference to the number of employees, the number of immigration enforcement agents involved in the incident, or the number of locations affected in a day."[354]

There are exceptions to each of these prohibitions. With respect to the prohibition against voluntary consent to enter non-public areas of the worksite, the provision on penalties does not apply if a court determines that the immigrant enforcement official entered the non-public area without consent of the employer or the other person in charge of the workplace.[355] In addition, the employer or a person acting of the employer's behalf is not precluded from taking the immigration enforcement officer to a non-public area where employees are not present for the purpose of verifying whether the agent has a judicial warrant.[356] This last exception only applies provided no consent to search non-public areas is given in the process.[357]

With respect to the subpoena or court order to access, review, or obtain employee records, the provision on penalties does not apply if a court determines that the immigration enforcement agent was permitted to access, review or obtain the employer's employee records without the consent of the employer or other person in control of the labor.[358] In addition, the law does not prohibit an employer from challenging the validity of a subpoena or judicial warrant in a federal district court.[359] The requirement of a subpoena or judicial warrant also does not apply to I-9 Employment Eligibility Verification forms and other documents for which a Notice of Inspection has been provided to the employer.[360]

With respect to the Notice of Inspection and posting requirements, "except as otherwise required by federal law," the employer must provide notice to each current employee of any inspections of I-9 Employment Eligibility Verification forms or other employment records conducted by an immigration agency.[361] The employer must give this notice "within 72 hours of receiving the notice of inspection" from the immigration agency, and the employer's notice to the current employees must be posted "in the language the employer normally uses to communicate employment-related information to the employee."[362] The employer must also give written notice "within 72 hours" to the employee's authorized representative, if any.[363] The posted notice must contain the following:

- The name of the immigration agency conducting the inspections of I-9 Employment Eligibility Verification forms or other employment records.
- The date that the employer received the notice of inspection.
- The nature of the inspection to the extent known.
- A copy of the Notice of Inspection of I-9 Employment Eligibility Verification forms for the inspection to be conducted.[364]

The California Labor Commissioner will be developing a template for posting that employers may use to comply with the requirements of notifying employees of an inspection of I-9 Employment Eligibility Verification forms or other employment records by an immigration agency.[365] The template will be posted on the California Labor Commissioner's Internet Web site.

In addition to providing current employees with written notice of the inspection, the employer must:

- Upon reasonable request, provide an affected employee with a copy of the Notice of Inspection of I-9 Employment Eligibility Verification forms.[366]
- Except as otherwise provided by federal law, provide each current affected employee and the employee's authorized representative (if any) with a copy of the following:
  - The results of the I-9 Employment Eligibility Verification forms or other employment records within 72 hours of receiving it[367]
  - Written notice of the obligations of the employer and the affected employee arising from the results of the inspection, within 72 hours of receiving the results.[368] The notice should relate to the affected employee only. It should be delivered by hand at the workplace if possible, and if not possible, by mail and email, if the email address of the employee is known. It also should be delivered to the employee's representative.[369] The notice should contain the following information:
    - A description of any and all deficiencies or other items identified in the written immigration results notice related to the affected employee
    - The time period for correcting any potential deficiencies identified by the immigration agency
    - The time and date of any meeting with the employer to correct any identified deficiencies
    - Notice that the employee has the right to representation during any meeting scheduled with the employer.[370]

An employer who fails to provide the above notices about the results of the inspection and what needs to be done to correct the deficiencies is subject to a civil penalty of two thousand dollars to up to five thousand dollars for the first violation, and five thousand dollars up to ten thousand dollars for each subsequent violation.[371] A penalty is not required to be imposed on an employer or person who fails to provide the notice to an employee at the express and specific direction or request of the federal government.[372]

C. ACCESS TO PERSONNEL RECORDS AND FILES IN LITIGATION

1. OVERVIEW

Requests for discovery of personnel files that occur during litigation raise issues of confidentiality and the employee's constitutionally protected right to privacy due to the personal nature of the information contained in personnel files. Therefore, in determining whether to allow disclosure of requested personnel files, "the party asserting a privacy right must establish a legally protected privacy interest, an objectively reasonable expectation of privacy in the given circumstances, and a threatened intrusion that is serious. [citations omitted.] The party seeking information may raise in response whatever legitimate and important countervailing interests disclosure serves, while the party seeking protection may identify feasible alternatives that serve the same interests or protective measures that would diminish the loss of privacy. A court must then balance these competing considerations." [373] Thus, disclosure of an employee's personnel file depends first on whether the material sought is relevant, and second, even if relevant, whether the policy in favor of discovery outweighs the individual's right to privacy in the contents of the material sought.[374] California courts have generally concluded that the public interest in preserving confidential information outweighs the interest of a private litigant in obtaining the confidential information.[375]

> ***El Dorado Savings & Loan Assoc. v. Superior Court*[376]**
> Plaintiffs, former female employees of El Dorado Savings & Loan, sought discovery of personnel records of a male employee, Morris, who was not a party to the lawsuit. Plaintiffs alleged that during the course of their employment, they were discriminated against on the basis of gender and age. Plaintiffs contended that disclosure was necessary to the prosecution of their discrimination case, since Morris was the only male employee working in the same capacity as plaintiffs and had allegedly received benefits not afforded plaintiffs.
>
> The Court of Appeal denied plaintiffs' discovery request for the disclosure of Morris' entire personnel file. The Court stated that consideration should be given to whether the information could be obtained by less intrusive means, such as deposing the person. The Court further stated that if no less intrusive means are available, the judge should examine the personnel file and disclose only information he/she determines is relevant to the lawsuit.

Moreover, parties or witnesses also may not discuss confidential information maintained in personnel files that is not otherwise discoverable. For example, a person who has knowledge of the information may not be asked to orally disclose it at deposition or trial.[377]

While it is not always clear in advance what would be allowable discovery, there are guidelines and procedures that can be followed depending on whom is making the discovery request and what information is requested.

2. ELECTRONICALLY STORED INFORMATION

Public entities that find themselves parties to litigation should also be wary of those rules of civil procedure that permit discovery of "electronically stored information."

The Federal Rules of Civil Procedure may affect information retention and storage policies of public entities.[378] The rules require each party to litigation to conduct an exhaustive search of all electronically stored information "in the possession, custody, or control of the party" and to disclose this information, except for privileged information, "without awaiting a discovery request." Disclosure is not limited to hard copies of emails or other electronically stored and transmitted information, and may include back-up tapes, employee PCs, and smartphones as well as electronic records of conversations through voice mail, text or instant messaging. While entities are protected from sanctions under the rules for deleting email and other electronically stored information as part of a "routine, good-faith operation," what constitutes a "routine, good-faith operation" has not been defined under the rules.

Similarly, the Electronic Discovery Act ("Act"), including section 1985.8. establishes procedures to obtain discovery of electronically stored information for litigants in California state courts and largely tracks the Federal Rules of Civil Procedure. The Act set forth procedures for objecting to the specified form or forms of producing the electronically stored information requested by the subpoena.

Anytime an entity is sued in federal or state court or has notice of a potential claim, it should preserve all electronic information regarding key player in the case or information that pertains to claims or defenses, or other relevant matter, in the case. The entity's efforts to preserve this information should include disabling the destruction of relevant electronically stored information pursuant to the entity's document retention policies. The entity should work with its IT department to determine the best manner in which to preserve its electronically stored information. The entity would not be sanctioned if the email or other electronically stored information was destroyed before the entity knew or had reason to know about a lawsuit or claim that required that it preserve that evidence. However, once the entity has knowledge of a claim or lawsuit, it must preserve that evidence; a Court could order evidentiary and/or monetary sanctions against the entity if the electronically stored information is destroyed.[379]

Thus, entities in litigation in either federal or state court should disable destruction of electronically stored information retention policy may find their policies tested under these discovery rules, and should install provisions into their policy that allow for a freeze on the destruction of any such information that may be pertinent to the litigation. In addition to freezing the terminating mechanisms on their work computers, public entities should instruct their IT department to save all backup tapes regarding information stored on and/or produced by key employees in the litigation. Public entities should discuss with their IT departments the best manner in which to preserve their electronically stored information pertaining to litigation.

3. EEOC/DFEH REQUESTS FOR INFORMATION

Public employers often find themselves presented with requests for employee personnel records by governmental agencies empowered with duties of investigation. The California Department of Fair Employment and Housing and the Federal Equal Employment Opportunity Commission often request such files in connection with investigation of discrimination, harassment or retaliation complaints. These requests often have a potential for violating employees' privacy rights. Failure to cooperate, however, may result in adverse consequences or impact upon the employer.

The courts have generally held that an employee's privacy rights are not violated when his or her personnel records are released to an investigatory agency constrained by confidentiality requirements. For additional protection, any disclosure of personnel files or information of uninvolved employees should be accompanied by a statement regarding confidentiality and a notice of liability of unauthorized disclosure. The statement and notice should read substantially as follows:

Sample Employer Statement of Confidentiality

(Employer) objects to producing the records or files of (Employee) on the grounds that such records or files are protected by the employee's right to privacy. Without waiving these privacy rights, (Employer) will supply the requested information with the understanding that (requesting agency) will keep these records confidential. Any failure to do so on the part of (the agency) or any of its employees will be the responsibility of (the agency), and by acceptance of these records, (the agency) agrees to maintain the records' confidentiality and hold the (Employer) harmless from any unauthorized disclosure.

***University of Pennsylvania v. EEOC*[380]**

In this case, the United States Supreme Court held that the University of Pennsylvania was required to comply with a discovery request from the Equal Employment Opportunity Commission (EEOC) for the tenure review files of a professor who filed a discrimination claim with the EEOC, and against the University.

The professor, Rosalie Tung, alleged that she had been denied tenure because the University did not want a Chinese-American woman in their school. She alleged that her qualifications were equal to or better than five named male faculty members who had received more favorable treatment.

The EEOC undertook an investigation of Tung's charge and requested a variety of information from the University. The University refused to provide Tung's tenure-review file, and the tenure files of the five male faculty members identified in the charge. The University claimed that "confidential peer review information" should not be released, because it would destroy the ability to give candid evaluations of young professors for fear of being dragged into a lawsuit.

The Supreme Court held that a charging party need only make a showing of relevance before peer review materials pertinent to charges of discrimination in tenure decisions must be disclosed. A higher standard, the Court held, would give employers a weapon to frustrate investigations.

4. SUBPOENAS FOR PERSONNEL RECORDS

A frequent question for employers is whether to release personnel records pursuant to a subpoena or other form of discovery demand. The Legislature has addressed privacy concerns relating to producing confidential records of others pursuant to the judicial subpoena process. California Code of Civil Procedure Section 1985.3 sets forth some specific employee notification requirements. These requirements are generally applicable to public sector personnel records (except for peace officers, as discussed *infra*) when such records are exempt from disclosure under the Public Records Act.[381]

Section 1985.6 requires a party obtaining a subpoena for personnel records to serve a copy of the subpoena and a "Notice to Consumer" upon the employee prior to the date set for production of the records. The agency official who is the custodian of the records must receive proof of either personal service or timely service by mail of the subpoena and the Notice to Consumer upon the employee otherwise the subpoena is defective and may not be enforceable.

The Notice to Consumer should read substantially as follows:

Sample Notice to Consumer Language

"PLEASE TAKE NOTICE that records concerning you are being sought from (name of the person or entity requesting the documents), named with the subpoena served with this notice. If you object to (name of the person and/or agency in custody of the records) furnishing copies of these records to the parties in this action, you must do one of the following prior to the date set for production:

1. Obtain the written agreement of (name of the person or entity requesting the documents) to cancel or limit the subpoena;

2. File a written motion with the Court to prevent or limit production of your records;

IF YOU CANNOT OBTAIN THE WRITTEN AGREEMENT of the party seeking your records to cancel or limit the subpoena, you should consult an attorney immediately to assist you in protecting your rights of privacy."

If the consumer records provisions are complied with and a subpoena otherwise appears to be properly issued and prepared, and if the employee does not object within the statutory period, an employer can usually legally release the records. However, in recognition of the privacy issues discussed above, it is advisable to consult with an attorney prior to releasing employee personnel records pursuant to a subpoena.

LCW Practice Advisor

Code of Civil Procedure Section 1985.3(a)(3) provides that neither (a) state or local agencies as defined by Government Code Section 7465 nor (b) California State Courts or entities created under Article VI of the California Constitution fall under the definition of "subpoenaing party." However, one court has held that a county had to provide a notice to consumer before it subpoenaed a plaintiff's medical records.[382] We thus recommend that state and local agencies comply with the notice to consumer requirements to avoid any issues that may arise if the affected individual challenges the discovery request.

5. DISCOVERY OF POLICE RECORDS

Police officers' personnel files are afforded greater protection than other public employees' files are given. In *Pitchess v. Superior Court*[383] the California Supreme Court explored the limits of discovery and disclosure of police personnel records. The Court held that a Sheriff Department's internal affairs investigation files of excessive force citizen complaints were discoverable. The defendant had shown **by affidavit** that the records sought were relevant to the criminal defendant's self-defense claim.

The Legislature has codified and expanded upon the *Pitchess* principles in Penal Code Sections 832.5, 832.7, 832.8, and Evidence Code Sections 1043 through 1047. Penal Code Section 832.7 provides for confidentiality of police officer personnel records and records of citizen complaints. The records are discoverable only pursuant to Evidence Code Section 1043 which requires the filing of a written motion with statutory notice (at least 21 days). The motion required under Evidence Code Section 1043 has come to be called a "*Pitchess*" motion, and the procedure is applicable in both criminal and civil matters. An attorney should be consulted **immediately** upon receipt of a *Pitchess* motion.

The declarations supporting the motion must demonstrate that the information sought from the police officer's records will facilitate the ascertainment of facts and a fair trial.[384] The allegations may be made on "information and belief" with reasonable particularity as long as the agency is not claiming the records are protected by an official privilege.[385] Evidence Code Section 1045(b) excludes the following records from discovery:

- Complaints more than 5 years old;
- Conclusions of any officer investigating a complaint; and
- Facts so remote as to make disclosure of little or no practical benefit.

This statutory scheme carefully balances the peace officer's claim to confidentiality and the criminal defendant's equally compelling interest in all information pertinent to the defense.[386]

***People v. Mooc*[387]**

A case which the California Supreme Court described as generating, "...no small amount of excitement from various governmental entities and organizations across the State...," the Court held that documents clearly irrelevant to a defendant's *Pitchess* motion need not be presented to the trial court for in camera review.

Defendant Mooc was charged with committing battery on a custodial detention officer in the employ of the City of Santa Ana. A broad *Pitchess* motion was filed seeking production of records of complaints, disciplinary actions and witnesses regarding alleged inappropriate use of force by the detention officer, and any and all documents defined by Penal Code §832.8 as constituting personnel records, including any psychological records. Following the in camera examination, the court ruled that the personnel file material produced for examination had, "...very little, if any, probable value, and based on that and §1045 of the Evidence Code, the court is going to decline allowing the defendant to peruse the officer's personnel records."

Following his conviction, the defendant appealed and moved that the Court of Appeal augment the record in the case by including those personnel records which were produced at the trial-level *Pitchess* proceeding. After being provided with a significantly greater volume of documents than were apparently provided to the trial court, the Court of Appeal reversed the conviction and ordered the trial court to conduct a new in camera hearing where the **complete personnel file** was subject to the in camera review.

The Supreme Court reversed, holding among other things, that that the custodian of records is not always required to produce the **entire personnel file** in response to a *Pitchess* motion. Additionally, the Supreme Court also established a detailed, proper method for reviewing a challenged *Pitchess* process.

a. Determining Relevancy of Documents

When served with a *Pitchess* motion, the custodian of records should engage in the following analysis to determine which documents should be presented to the trial court if an in camera review is ordered. Only those peace officer personnel records that are relevant to the subject matter involved in the pending case should be presented. For example, although records relevant to a criminal case involving a battery on an officer will generally consist of documentation regarding complaints of excessive force, those records would likely be irrelevant in a civil proceeding where the plaintiff's allegations consist of negligence by an officer in operation of a motor vehicle.

The analysis is as follows:

- Carefully read the *Pitchess* motion and its attachments in order to determine the nature of the documents that are relevant to the particular proceeding which is the subject of the motion.
- If the custodian of records has any doubt whether a particular document is relevant, he or she should present it to the trial court if an in camera hearing has been ordered.
- If the custodian of records determines that any personnel documents are clearly irrelevant to the proceeding, those documents need not be presented for an in camera review, but the custodian should be prepared to state in chambers and for the record what those withheld documents consist of and why they were deemed by the custodian to be irrelevant or otherwise non-responsive to the *Pitchess* motion.

In determining which documents are relevant for production in an in camera review, custodians of records should be mindful of the Supreme Court's holding that, "...if the custodian has **any doubt** whether a particular document is relevant, he or she should present it to the trial court." On the other hand, in the overwhelming majority of cases, documents regarding marital status, family member identification, employment application information, letters of recommendation, promotion records and health records, need not be produced for an in camera review, **unless the same are relevant to the particular case pending before the court.** Where any particular *Pitchess* motion presents a "close call" on the issue of document relevancy, it is recommended that the custodian consult with appropriate legal counsel as an aide in making the relevancy determination.

b. Exclusions

The confidentiality sections of the Penal Code Section 832.7 and Evidence Code Sections 1043 and 1045 do not restrict access by the California Attorney General or a grand jury in the course of an investigation of an officer's or policy agency's conduct.[388]

Penal Code section 832.7 does not create a privacy interest on the part of individual witnesses or officers in tapes and transcripts of witnesses interviewed during police commission's investigations of employment discrimination charges against a police officer.[389]

When a former police officer testifies against a police department in a lawsuit, the police department which employed the officer may allow its lawyer to review the former police officer's personnel file in order to evaluate its use during cross-examination and as impeachment at trial without complying with the *Pitchess* procedural requirements and without violating the officer's right to privacy.[390]

In addition, the names, employing departments, and hiring and termination dates of peace officers maintained by the California Commission on Peace Officer Training and standards do not constitute confidential peace officer personnel records under Penal Code Sections 832.7 and 832.8.[391] Similarly, "well-established norms of California public policy and American public employment exclude public employee names and salaries from the zone of financial privacy protection." Thus, the names and salaries of public employees earning $100,000 per year or more, including peace officers, are not protected from disclosure as personnel records under Penal Code sections 832.7 and 832.8.[392]

D. EMPLOYER'S OBLIGATION TO PREVENT IDENTITY THEFT

The Fair and Accurate Credit Transactions Act require that all "creditors" (including local government agencies that defer payments for goods or services) have policies and procedures in place to help prevent identity theft.

1. SECTION 114 OF THE FACT ACT

Section 114 of the Act requires that each "creditor" that offers or maintains "covered accounts" develop and implement an Identity Theft Prevention Program (ITPP) for combating identity theft in connection with new and existing accounts.

a. Complying with the Red Flags Rules

To comply with the FACT Act regulations, known as the Red Flag Rules, entities will be required to provide for the identification, detection, and response to patterns, practices, or specific activities ("red flags") that could indicate identity theft in their identity theft prevention programs.

The Red Flags Rules apply to "creditors" with "covered accounts." Under the Red Flags Rules, creditors must develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of

Directors or senior employees of the creditor, include appropriate staff training, and provide for oversight of any service providers.

A "creditor" includes government entities which defer payment for goods or services (for example, payment for utilities or payment plans for parking tickets). "Deferring payments" refers to postponing payments to a future date and/or installment payments on fines or costs. A "covered account" is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account includes an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

b. What are Red Flags?

The Red Flags Rules provide all creditors the opportunity to design and implement a program (ITPP) that is appropriate to their size and complexity, as well as the nature of their operations.

The Federal Trade Commission has identified 26 examples of red flags. These red flags are not a checklist, but rather, are examples that creditors may want to use as a starting point. The 26 red flags fall into five categories:

1) Alerts, notifications, or warnings from a consumer reporting agency (for example, a fraud alert included with a consumer report);

2) Suspicious documents (for example, documents provided for identification that appear to be forged);

3) Suspicious personally identifying information (for example a suspicious address, or a social security number has not been provided, or is listed on the SSA's Death Master File);

4) Unusual use of – or suspicious activity relating to – a covered account (for example, a material change in purchasing or spending); and

5) Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

c. *Drafting The ITPP*

The ITPP must include the following four basic elements for detecting, preventing, and mitigating identity theft and enable a creditor to:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the ITPP is updated periodically to reflect changes in risks from identity theft.

There are also certain steps that a creditor must take to administer the ITPP: obtaining approval of the initial written ITPP by the board of directors, or if none, then by an appointed senior manager/employee of the creditor; ensuring oversight of the development, implementation and administration of the ITPP; training staff on the ITPP; and overseeing service provider arrangements.

2. SECTION 315 OF THE FACT ACT

Section 315 of the Act also requires issuers of debit or credit cards to assess the validity of a change of address if they receive notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterward they receive a request for an additional or replacement card for the same account (this will not typically apply to our public agency clients).

In addition, Section 315 amended Section 605 of the FCRA, 15 USC 1681(c), by adding a new subsection (h). Section 605(h)(1) requires users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency (i.e., when an address provided by a consumer "substantially differs" from the one the credit reporting agency has on file). Our public agency clients may be users of consumer reports (for example, when conducting background checks), so they should have a policy in place to (1) enable the employer to form a reasonable belief that the employer knows the identity of the person for whom it has obtained a consumer report, and (2) reconcile the address of the consumer with the credit reporting agency, if the employer establishes as continuing relationship with the consumer and regularly, and in the course of business furnishes information to the credit reporting agency.

3. THE CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act of 2018 gives California residents ("consumers") the right to: (1) know what personal information a business has about them, and where information came from or was sent (e.g. who it was sold to); (2) delete personal information that a business collects from them; (3) opt-out of the sale of personal information about them; and (4) receive equal service and pricing from a business, even if they exercise their privacy rights under the law, with some exceptions.

Companies will need to provide information to consumers about these rights in privacy policies and will need to provide consumers with the ability to opt out of the sale of personal information by supplying a link titled "Do Not Sell My Personal Information" on their home page. The Act further provides that a business must not sell the personal information of consumers younger than 16 years of age without that consumer's affirmative consent or for consumers younger than 13 years of age, without the affirmative consent of the consumer's parent or guardian.

The Act defines "personal information" broadly as any information that identifies or can be used to identify a consumer or their household, such as: records of products purchased, browser search histories, educational information, employment history, and IP addresses.

Public entities do not need to comply because the law only applies to: for-profits doing business in California, that (a) have annual gross revenues in excess of $25 million; or (b) receive or disclose the personal information of 50,000 or more Californians; or (c) derive 50 percent or more of their annual revenues from selling California residents' personal information.

However, when contracting with covered companies, public entities will want to ensure that the obligations and risks of the law rest squarely with the for-profit business. Those risks are real. The Attorney General has enforcement authority over the Act. Consumers may bring class actions against non-compliant companies that allow sensitive consumer personal information to be stolen or wrongfully disclosed. In these cases, consumers may seek statutory damages between $100 and $750 per California resident per incident.

Legal snapshot: Employee Searches and Surveillance	
Applicable laws:	• Constitutional Right of Privacy (Cal. Const. art. I, § 1) • Fourth Amendment of the U.S. Constitution • Public Safety Officers' Procedural Bill of Rights Act, Cal. Gov. Code §§ 3300 *et seq.* • Various other federal and California statutes • Common law torts
Who and what is protected?	• All current employees • Employee's person, personal property, and those personal work areas and activities in which there is a reasonable expectation of privacy
Generally, employers must NOT:	• Search employee's person or personal property • Search employer property or areas unless there is: a) a reasonable suspicion of workplace misconduct; and b) a reasonable belief that the search will turn up evidence supporting the suspicion.
The balancing test for this is:	• Employee's reasonable expectation of privacy versus employer's legitimate interest in maintaining a safe and efficient workplace or "the realities of the workplace"

A. SEARCHES OF WORK AREAS

1. EMPLOYEES IN GENERAL

Searches of public employee property, desks, lockers, and work areas implicate employees' privacy rights as well as Fourth Amendment rights. The courts have held that employees have a reasonable expectation of privacy in areas that they intend to maintain as private depending upon the "realities of the workplace." At the same time, employers have a legitimate interest in maintaining a safe and efficient workplace.

As noted previously, in 1994, in *Hill v. NCAA*, the California Supreme Court adopted a new "balancing test" approach for analyzing state constitutional privacy claims. This standard is less stringent than the "compelling interest" standard, which under *Hill*, only applies in limited circumstances. Neither the precise scope of each of these standards, nor the extent of an employee's privacy rights in a workplace setting are entirely settled. The result may depend on the public interest, the employer's special interests, and the employees' reasonable expectations of privacy in a particular employment setting.

Ortega v. O'Connor

On appeal from the District Court after remand from the United States Supreme Court, the Ninth Circuit Court of Appeals held that a public employee's Fourth Amendment rights were violated when his office was searched without a warrant and personal materials were seized in response to vague and very old allegations of sexual misconduct.[393]

Dr. Magno Ortega held the position of Chief of Professional Education at Napa State Hospital from 1964 to late 1981. In 1981, he purchased a new computer to be used in his program by obtaining donations and contributing approximately half the cost of the computer himself. Based on concerns regarding the computer purchase, the hospital began an investigation into Ortega's management practices. During the investigation, it was alleged by a staff psychiatrist that Dr. Ortega had engaged in sexual harassment of resident physicians.

Subsequently, Ortega's office was searched without a warrant. The documents searched and read included personal letters from friends and family, as well as sexually explicit letters from several women. Personal possessions as well as state property were boxed and removed. Based on the investigation, Ortega was fired. He filed a complaint in 1982 under Title 42 United States Code section 1983, alleging violations of his Fourth Amendment rights to be free from unreasonable search and seizures. This lawsuit eventually reached the United States Supreme Court becoming the seminal case on employee privacy rights in the workplace.[394] The United States Supreme Court held that work-place searches "should be judged by the standard of reasonableness under all the circumstances," in which "both the inception and the scope of the intrusion must be reasonable."[395] The United States Supreme Court remanded the case to the District Court for further proceedings and a jury found in favor of Ortega, awarding him $376,000 in compensatory damages plus punitive damages. Another appeal followed, extending the length of this litigation to approximately sixteen years.

The Court of Appeals affirmed the District Court's decision on remand.[396] The Court held that the search and seizure of the personal materials would only be lawful in the context of a search regarding allegations of sexual misconduct. The type of materials taken from Ortega's office, i.e., truly private papers or

communications, lie at the core of the First and Fourth Amendment. The allegations of sexual harassment were so old and vague that they could not serve as a basis for reasonable suspicion warranting a search of the employee's private office, let alone such an intrusive search of his personal materials. Moreover, the Court held that there was no reasonable suspicion that the evidence of sexual harassment would be found in Ortega's office.

Even if a search does not violate an employee's right to privacy, this does not always mean that the information or "evidence" obtained in such a search can be used. In some situations, there are other considerations that preclude use of information obtained in the course of a lawful search. Thus in *People v. Jiang* (originally published at 131 Cal.App.4th 1027, but subsequently ordered to be not officially published) the trial court found that information stored on a laptop computer provided by a criminal defendant's employer was not protected by the attorney-client privilege because the employee-defendant had no reasonable expectation of privacy as to that information. The basis for the trial court's ruling was the employer's written computer use policy that advised the employee-defendant that information stored on the computer remained that of the employer and was subject to inspection. The employee even signed the policy affirmatively acknowledging that he had no reasonable expectation of privacy in any information he placed on the computer. The information in question included notes and other materials the employee prepared for and with his attorney in connection with the criminal charges filed against him. The Court of Appeal reversed holding that notwithstanding the employee's lack of any reasonable expectation of privacy, the information in question was protected from disclosure by the attorney-client privilege. *Jiang* is not citable authority because of the California Supreme Court's order that it not be published. However, the Court of Appeal's ruling is consistent with authorities across the country that seem to uphold the application of privileges to material otherwise found to be not private.

***City of Ontario v. Quon*[397]**

The United States Supreme Court unanimously found that the City of Ontario's Search of its employee text messages on a City provided pager was reasonable and did not violate the employee's Fourth Amendment Rights.

The City of Ontario contracted with Arch Wireless to provide alphanumeric text-messaging pagers to members of the Police Department's Special Weapons and Tactics (SWAT) Team. The City intended the pagers to help the SWAT employees mobilize and respond to emergency situations. The Arch Wireless network and equipment transmitted and archived messages received and sent by the employees on Arch Wireless pagers. The text messages did not pass through the City's computers, and thus, the City did not have access to the content of the messages.

Under the City's contract, each pager was allotted a limited number of characters per month. The City was billed overage charges for each pager that exceeded the monthly allotted character amount.

While the City did not have a written policy concerning the use of text-messaging pagers, it did have a general "Computer Usage, Internet and E-mail Policy" ("the policy") that put all employees on notice that City-owned computers and equipment were to be used solely for City related business. The City told employees in a staff meeting and in a memorandum that text messages fell within the City's policy as public information and would be subject to auditing.

Quon and other officers exceeded their allotted characters for a number of months and were allowed to reimburse the City. Later, the Chief decided to audit the usage to determine if the allotted character under the City's contract with Arch Wireless was sufficient. The City obtained transcripts directly from Arch Wireless, and determined that the vast majority of Quon's usage was personal, not City-business. Quon was investigated and disciplined. Sergeant Quon, his wife, and other employees filed a complaint against Arch Wireless alleging violation of the Stored Communication Act, 18 U.S.C. §§ 2701-2711 (1986), and against the City, the Police Department, and the Chief for violation of their right to be free from unreasonable searches and seizures pursuant to the Fourth Amendment to the United States Constitution, and violation of their privacy rights under Article 1, Section 1 of the California Constitution. The parties filed several summary judgment motions. The District Court denied the plaintiffs' summary judgment in full, and granted in part and denied in part the City and Arch Wireless' summary judgment motions.

On appeal, the Ninth Circuit Court of Appeals held that the search of the text messages violated the appellants' Fourth Amendment and privacy rights because they had a reasonable expectation of privacy in the content of the text messages, and because the search was unreasonable. The court also held that Arch Wireless violated the Stored Communications Act because, as an electronic communications service, its release of the private data required the lawful consent of either the addressee or the recipient of the communications (as the subscriber, the City did not have a right to access the communications).

The City appealed the Ninth Circuit's ruling and the United States Supreme Court agreed to decide the Fourth Amendment questions. The Supreme Court decided this case without determining whether Quon had a reasonable expectation of privacy in the text messages. The Supreme Court discussed the difficulty in predicting how employee privacy rights will be shaped by the rapid evolution of technology used to communicate, society's workplace norms, and laws protecting employee rights, The Court was thus reluctant to issue a broad holding concerning employees' privacy expectations vis-à-vis employer-

provided technological equipment for fear of the implications such a holding would have on future cases.

Because this case could be decided on narrower grounds, the Supreme Court made three assumptions for the sake of argument: (1) that Quon had a reasonable expectation of privacy in the text messages sent on the City issued pager; (2) the City's review of the transcript constituted a Fourth Amendment search; and (3) principles applicable to a public employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.

The Supreme Court found that the search was justified at its inception because there were reasonable grounds for suspecting that the search was necessary for noninvestigatory or administrative purposes. Specifically, the Police Chief ordered the search to determine whether the character limit on the City's contract was sufficient to meet the City's needs. The City had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses. On the other hand, the City had to determine whether it was paying for extensive personal communications.

The scope of the City's search was also reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use. Although it may have been reasonable for the City to review transcripts of all the months in which Quon exceeded his character allotment, the City only reviewed the messages for two months. The investigation was also limited to the review of a redacted transcript covering only messages Quon sent while on duty.

Even if Quon had some expectation of privacy in his messages, the Supreme Court held that it would not have been reasonable for Quon to believe that his messages were in all circumstances immune from scrutiny. The Department had told him his messages were subject to auditing. As a law enforcement officer, he knew or should have known that his text messages could be reviewed to assess the SWAT Team's performance in particular emergency situations or some other legitimate purpose. Although there were arguably less intrusive searches available, the Court rejected the suggestion that the City was required to use the least intrusive means to reach its goal.

Finally, the Court found that because the other respondents' claims hinged on a determination that the search was reasonable as to Quon, their Fourth Amendment claims also failed.

Because the Supreme Court did not determine whether Quon had a reasonable expectation of privacy over his text messages, this case should serve as a reminder to employers that they should adopt written policies that put employees on notice that they do not have an expectation of privacy in their electronic communications sent or received via employer property. The policy should also use language broad enough to encompass current and emerging forms of electronic communications used in the workplace.

Notably, the Court's decision only reviewed the Fourth Amendment arguments. The Court did not grant certiorari to review the Ninth Circuit's holding that Arch Wireless violated the Stored Communications Act by providing the City with transcripts of Quon's text messages. Thus, that portion of the Ninth Circuit's decision stands. Because the Stored Communications Act prohibits third party Electronic Communications Services from disclosing archived messages except to an addressee or intended recipient of such communication, we recommend that employers obtain a written and signed release from all employees that allows the employer access to such communications before they issue the equipment to employees.

Crispin v. Christian Audigier, Inc.[398]
A federal district court in California held that Stored Communication Act prohibits "electronic communication service providers" from divulging, either voluntarily or in response to a subpoena, private messages communicated via social networking sites that are not readily accessible to the public.

Riley v. California[399]
The United States Supreme Court unanimously found that law enforcement must generally obtain a search warrant before searching digital information contained on a cell phone seized from an arrested individual.

Riley involves two cases, one involving a smartphone and the other involving a flip phone. In each case, an individual was arrested for allegedly violating the law and as part of the arrest, his cell phone was seized. The officers in each case conducted warrantless searches of the cell phones and uncovered information that exposed additional criminal activity.

In one case, the content of the seized smartphone revealed text messages with possible gang affiliations, videos of young men sparring while someone yelled gang words, and a photograph of the arrestee in front of a car suspected to have been involved in a shooting a few weeks earlier. The arrestee was linked to the prior shooting based upon the information found on his cell phone.

In the other case, the flip phone seized from the arrestee repeatedly received calls from a source identified as "my house" on the phone's outside screen. When the officers opened the phone, they saw a photograph of a woman with a baby set as the phone's wall paper. The officers were able to trace the phone number of the caller to an apartment building where, from the picture of the woman on the phone, they were able to locate the place where the arrestee lived. After securing the apartment and obtaining a warrant, they found and seized cash, a large quantity of drugs, and a firearm with ammunition.

Both arrestees sought to suppress the evidence uncovered through the search of their cell phones on the grounds of an unlawful search and seizure under the Fourth Amendment. The U.S. Supreme Court agreed with the arrestees, finding that the warrantless search of their cell phones incident to their arrests was not reasonable. In evaluating the reasonableness of the warrantless search incident to the arrest, the Court declined to apply the rules previously applicable to the search of physical objects found on or near the arrestee during his or her arrest.

The Court ruled that cell phones differ both quantitatively and qualitatively from the typical physical object that might be found on an arrestee during an arrest. Of particular note was the immense storage capacity of a cell phone, which permitted individuals to carry around vast quantities of sensitive personal information that they would not have been able to carry on their person separately without a cell phone. Thus, rules that previously permitted the warrantless search of physical items incident to the arrest and that resulted in searches that were narrow in scope due to the physical limitations of the items being searched, would not apply to cell phones. Just as an officer would need a search warrant to search a trunk found incident to an arrest, the officers would also need a search warrant to search a cell phone, which would require a trunk to hold the same number of physical pieces of information found on the cell phone.

The Court also rejected the arguments of the respondents that reasons of safety and the need to prevent destruction of evidence permitted a warrantless search of the cell phone. Respondents did not offer evidence based upon actual experience that arresting officers faced harm at the time of the arrest unless they searched the cell phone without a warrant. With respect to arguments on the destruction of evidence, the Court found that steps could be easily taken prior to an arrest to remotely wipe or encrypt data and prevent officers from accessing the phone. In the event the phone was unlocked and accessible to the officer at the time of the arrest, the officers could take simple steps to prevent the phone from being remotely wiped or data encrypted, such as turning off the phone, removing its battery, or keeping the phone powered on and placed it in a Faraday bag that isolates the phone from radio waves.

The Supreme Court's decision in *Riley* established an important privacy interest. This case will likely influence court decisions in civil cases involving discovery issues or investigations where information is sought from a personal smartphone.

Williams v. Superior Court[400]
Court permitted discovery of names and address of other employees who may have an interest in a class action to recover wages on their behalf over assertion of privacy objections raised by the employer. Court explained that not ever assertion of a privacy interest under the California Constitution must be overcome by a compelling interest. A compelling interest is only required for "an obvious invasion of an interest fundamental to personal autonomy." However, "when lesser interests are at stake," a "more nuanced framework" applies, "with the strength of the countervailing interest sufficient to warrant disclosure of private information varying according to the strength of the privacy interest itself, the seriousness of the invasion, and the availability of alternatives and protective measures."[401]

2. PUBLIC SAFETY OFFICERS

Under the Public Safety Officers Procedural Bill of Rights Act, the agency may not search an officer's locker or personal storage space except in the officer's presence, or with his or her consent, or unless a valid search warrant has been obtained, or where he or she has been notified in advance that a search will be conducted.[402]

However, an office or locker search of space under the employer's control may still violate the constitutional restriction on unreasonable search or seizures if the employee has a "reasonable expectation of privacy." As with other employees, if this is the kind of area that is subject to searches on a normal basis, then the employee's reasonable expectation of privacy may be diminished.

The department may not coerce an administrative search of locations other than those under departmental control. If the department wishes to avoid the possible exclusion of evidence when searching locations such as an officer's vehicle or home, as well as a possible lawsuit for violation of civil rights, it must obtain the officer's consent or a valid search warrant. If an officer is forced to comply with an order to permit a search to avoid a possible charge of insubordination, the officer may have grounds for the exclusion of the evidence obtained as well as a civil lawsuit. For example, a federal court has held that a police officer is not required to open his home whenever reasonable suspicion exists that evidence may be found. Under such circumstances, an administrative warrant is improper and constitutionally infirm.[403]

3. CHECKLIST: GUIDELINES FOR CONDUCTING SEARCHES

- ❑ Retain a key or combination for each locker, desk or vehicle on agency property and notify the employees of this fact. Make sure any lock on agency property is owned and supplied by the employer and forbid employees to use their own locks.
- ❑ Provide formal notice to employees that lockers, desks and vehicles may be searched without employee consent or knowledge and that refusal to permit such searches may result in discipline.
- ❑ Prepare a written policy concerning searches and have each employee sign a written acknowledgment stating that the employee has received and read the written search policy.
- ❑ Secure a valid search warrant prior to conducting a search at the request of the police
- ❑ Conduct searches in an evenhanded and nondiscriminatory manner.
- ❑ If possible, obtain consent of the employee before conducting the search.

B. SEARCHES OF EMPLOYEES AND EMPLOYEE PROPERTY

The searching of persons and property is normally a function of law enforcement. Employer searches are fraught with potential hazards that can ultimately result in sizeable damage awards in favor of employees. Even where an employer has reasonable suspicion or probable cause to believe that an employee may have an item or a substance prohibited by law or policy in his or her possession, or in his or her automobile, the employer should not search an employee or an employee's personal possessions. Employers have several other options:

- Ask the employee to submit voluntarily to being searched or to have his or her possessions searched.
- Call local law enforcement and allow them to search if they determine that it is appropriate.
- Prevent the employee from continuing to work and send the employee home.
- Prepare to institute disciplinary action against the employee.

Unless an item or a substance in violation of the established policy is in plain view of management personnel so it can be seized without a search, management personnel should consult with legal counsel and/or human resources professionals before conducting a search since managers/supervisors are generally not trained in how to pat search or fully search an individual. Improperly conducted searches can lead to altercations, ill will and lawsuits.

Employers may, however, search areas where the public agency maintains full control or joint control with the employee. For instance, it would be permitted to search an agency vehicle that an employee operates during working hours but does not take home. Or, it would be permissible to search an employee's locker where both the employer and employee have a key. In either situation (or in similar situations) public agencies are best protected if they include in their

policies that employment constitutes permission to conduct such searches. Arguably, once employees are clearly notified that searches of such areas are possible, they will lose any legitimate expectation of privacy in the area or the possession. Even if an employee has an expectation of privacy in certain areas, the United States Supreme Court held in *O'Connor v. Ortega* that a search may be permissible if the employer had reasonable grounds for: 1) suspecting that the employee had engaged in workplace misconduct; and 2) believing that a search of these office areas would turn up evidence supporting that suspicion.[404]

In contrast, when an employee's personal possessions, such as a purse or lunch box, are located in an area such as a locker where the employer might otherwise have a right to search, the employer should not open the employee's personal possession without permission or assistance from law enforcement personnel.

> ***Finkelstein v. State Personnel Board*[405]**
> An employer found information in a personal briefcase, after it had warned employees to remove all confidential papers from their offices in preparation for an office move. The court allowed the contents of the briefcase to be introduced as evidence in an administrative disciplinary hearing, holding that the Fourth Amendment exclusionary rule did not apply. The court's reasoning turned on the fact that the search was motivated by the employer's desire to prepare to move the office rather than by the desire to uncover evidence damaging to the employee.

C. MONITORING OF ELECTRONIC COMMUNICATIONS

The advent of new forms of advanced communications technology has created a myriad of legal questions for public employers. Foremost among these issues is whether employers have the right to access emerging technologies such as voice and electronic mail messages generated or received by their employees. Employer monitoring of and access to voice and electronic mail, pagers, and text messages present significant employment privacy issues. Because it is common for employees to use employer issued communications devices, such as cellular telephones and computers, to send both personal and business-related messages, a host of legal questions arise.

While most employers will block employees from accessing harmful materials on the Internet via the employer network, including access to social networking sites, it is important that employers also educate their employees about appropriate and responsible behavior online during off duty hours. Employees should also be on notice via written guidelines about the consequences of inappropriate off-duty Internet behavior. Employer guidelines help educate employees about the importance of responsible behavior online.

Employers must be aware of federal and state authorities that protect electronic communications. This section provides an overview of these laws.

D. APPLICABLE FEDERAL LAW

1. REASONABLE EXPECTATION OF PRIVACY STANDARD APPLIES

The United States Supreme Court has determined that what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected under the Fourth Amendment's guarantee of freedom against unreasonable searches and seizures. In Katz v. United States, the court found the government's procedures constitutionally invalid when a telephone conversation was monitored by an electronic surveillance device attached to the outside of a public telephone booth where the defendant was prone to place interstate wagers from a particular telephone booth.406 The court concluded the Fourth Amendment "protects people, not places." The Fourth Amendment is now held primarily to protect "reasonable expectations" of privacy, including, as in Katz, conversations originating from a public telephone booth.

The question of whether an employee had a reasonable expectation of privacy in the workplace is resolved by examining whether the individual challenging the alleged intrusion had a subjective expectation of privacy which was objectively reasonable. If such an expectation is established, the inquiry then moves to the remaining issues raised by the Fourth Amendment. FN *United States v. Long* (2006) 64 M.J. 57.

In *Haynes v. Office of the Attorney General Phill Kline,*[407] Plaintiff was terminated from the position of assistant attorney general and sued the state Attorney General's Office and several co-workers seeking damages and injunctive relief from accessing his private files on his work computer contrary to his Fourth and Fourteenth Amendment rights and in violation of federal law. The District Court held that the plaintiff sufficiently alleged he had a subjective expectation of privacy in private files stored on his work computer, and that the expectation was objectively reasonable under the Fourth Amendment, so as to show likelihood of success on the merits in his claim for a preliminary injunction precluding his former employer from accessing, copying, reading, reproducing, disseminating, or otherwise searching his private files and e-mail communications.

According to the United States Supreme Court in *O'Connor v. Ortega*, work-related intrusions by public employers may be justified by the governmental interest in the efficient and proper operation of the workplace.[408] With respect to investigations of work-related misconduct, the *O'Connor* Court stated that:

> *Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practice and procedures, or by legitimate regulation. . . . Public employers have an interest in ensuring that their agencies operate in an effective and efficient manner, and the work of these agencies inevitably suffers from the inefficiency,*

incompetence, mismanagement or other work-related misfeasance of its employees.[409]

Employers do not have the right to eavesdrop on an employee's private telephone conversations. However, as explained below in greater detail, employers do have the right to control and monitor their electronic communications resources. To do so, employers must put their employees on notice by adopting a written policy that includes specific language advising employees that all electronic communications, including e-mail and text messages, sent and received on the employer's equipment, including cellular telephone, pagers, and other electronic devices are the employer's property and are subject to monitoring. Moreover, employers must consistently apply their written policy.

2. FEDERAL STATUTES PROHIBIT INTERCEPTION OF ELECTRONIC TRANSMISSIONS

The Federal Crime Control and Safe Streets Act of 1968 ("Wiretap Act")[410] makes it illegal to intentionally intercept any wire, oral or electronic communication without consent. The Electronic Communications Privacy Act ("ECPA") of 1986 amended the 1968 Wiretap Act. It prohibits intentional interception of electronic communications and disclosure or use of intercepted electronic communications during transmission (before the communication is open or stored).[411] It requires the presence of some federal nexus in its application (such as "the defendant acting under the color of state law or the recordings made through facilities of a communication carrier engaged in the transmission of interstate or foreign communications") to be constitutional as applied.[412]

The ECPA also created the Stored Communications Act ("SCA"), which prohibits intentional and unauthorized access of a facility providing electronic communication service to obtain "access to a wire or electronic communication while it is in electronic storage in such system."[413] The SCA also prevents "providers" of communication services from divulging private communications to certain entities and/or individuals.[414] The SCA provides privacy protection to communications held by two types of providers: electronic communication service ("ECS") and providers of remote computing service ("RCS").

An ECS provides its clients with wire or electronic communications services, such as e-mail. The Stored Communications Act prohibits an ECS from releasing the contents of a communication in electronic storage except to the sender or recipient of the communication.

On the other hand, an RCS provides its clients with computer storage or processing services "by means of an electronic communications system." For example, subscribers, such as banks or hospitals, may contract with an RCS for computer processing or storage of records. While the information is communicated electronically for storage or processing to an RCS, providing communications services is not the main purpose of an RCS. Under the Stored Communications Act, an RCS may release the contents of a communication with the lawful consent of a subscriber. Thus, for example, if an employer uses an RCS to store certain employee files, the employer as the subscriber has the right to access those employee files without the consent of the employee.

In *Quon v. Arch Wireless Operating Co., Inc*[415], the Ninth Circuit ruled that the employer's text message provider, Arch Wireless, violated the Federal Stored Communications Act, finding that it was an ECS, and thus, it could not release transcripts of employee text messages, sent and received via employer issued pagers, without the lawful consent of either the sender or the recipient of the communications. While the Supreme Court reversed other aspects of the Ninth Circuit's decision in *Quon v. Arch Wireless Operating Co.,* it did not grant review of the ruling that Arch Wireless violated the SCA. Therefore, that ruling remains good law.[416]

In *Quon*, the employer, a city, was the subscriber or contracting party with Arch Wireless, did not have the right to consent to the release of the text message transcripts. The Ninth Circuit rejected the trial court's finding that Arch Wireless was an RCS. Instead, it found that Arch Wireless' primary function was to send and receive electronic communications (by allowing users of the pagers to receive and send text messages) which fell precisely within the definition of an ECS. Arch Wireless stored the communications temporarily or for backup purposes; this type of storage by an ECS was contemplated under the Act. Arch Wireless did not provide the city with either "processing services" or "computer storage services," the primary functions of an RCS.

Generally, employers route and store their e-mail on their own servers and equipment. However, text messages, which are communicated via cellular telephones or pagers, are routed through a wireless communications provider (an ECS) which often only temporarily stores the record of the communication.

If an employer wishes to avoid the uncertainties that arise when messages, including e-mail, are routed through the network of an outside communication service provider, the employer may choose to limit its communication resources to those that are routed through the district's server and equipment. For example, certain cellular telephones have software that allows the employer to route all communications through its network.

Additionally, in light of the ruling in *Quon v. Arch Wireless*, companies in the business of providing electronic communications services will likely require a specific waiver from the end user of an electronic device (such as cellular telephones, personal digital assistants) as a condition of releasing information to the employer (the subscriber). For this reason, if the employer wants to monitor communications transmitted via ECS providers, it should obtain a signed release from all employees using employer issued pagers and cellular telephones that specifically allows the ECS provider to release the communications to the employer.

3. BUSINESS USE AND NOTICE EXCEPTIONS

Two exceptions to the Wiretap Act and the ECPA may apply to employers. The first is a "business exception" that allows operators of communication service providers to monitor the use of their equipment in the ordinary course of business for purposes of protecting their rights and property. For example, an employer that hosts its own e-mail service may monitor employee activity on its server.

Second, the Wiretap Act does not apply where a party to the electronic communication has consented to the interception. Thus, an employer who gives employees notice that their electronic communications are subject to monitoring, and has obtained each employee's written consent to monitoring through a signed acknowledgment of the employer's computer and electronic communications policy, has greatly insulated itself against potential liability.

Watkins v. L. M. Berry Co.
The employer had a policy of monitoring sales calls as part of its employee training program.[417] The court held that because of the company policy, the employer could monitor business calls without violating the Act.

Briggs v. American Air Filter Co. Inc.[418]
An employer was held not to have violated the Federal Wiretapping Laws by intercepting an employee's phone call who was disclosing confidential business information to a competitor.

Epps v. St. Mary's Hospital of Athens[419]
The employer was held not to have violated the law when she intercepted an interoffice phone conversation between two employees who were making scurrilous and disparaging remarks about fellow employees.

Bohach v. City of Reno[420]
Police officers claimed violations of the Fourth Amendment and wiretap statutes and sought to halt their Department's investigation into their possible misuse of the computerized paging system. The court held that the police officers did not have a reasonable expectation of privacy in their use of the computerized paging system and that the Department could access their electronic messages. The court stated that all the messages were recorded and stored, not because anyone was "tapping" the system, but simply because that was an integral part of the technology which stored messages in the central computer. Further, the Department had notified all users that their messages would be "logged on the network" and that certain types of messages were banned from the system.

United States v. Simons[421]
This case involved an employee's use of the Internet. Mark Simons was employed as an electrical engineer within the Foreign Bureau of Information Services ("FBIS") which is a part of the CIA. Simons had access to both a computer system, owned and operated by the CIA, and to the Internet. The CIA had an employee who managed the computer network for FBIS and who monitored the Internet traffic. The CIA conducted a search of which web sites were being frequented from their computer network and determined that Mark Simons was frequenting pornographic sites and that he had downloaded 1,000 documents that were pornographic in nature.

Simons moved to suppress this evidence claiming that the CIA had conducted an illegal search in violation of his Fourth Amendment rights since the search was conducted without a warrant or other lawful justification. The court held that Simons did not have a reasonable expectation of privacy with regard to any Internet use since his employer had an official policy regarding such use which stated that official business use, incidental use, lawful use and contractor communications were permitted and that audits would be implemented to support identification, termination and prosecution of unauthorized activity and that audits would be capable of recording the various web sites visited by employees.

United States v. Zeigler[422]
A private employer, cooperating with a federal investigation, turned over to the FBI the contents of an employee's workplace computer hard drive, which was found to contain child pornography. In a subsequent criminal proceeding, the employee sought to suppress the evidence on the basis that it allegedly resulted from a search in violation of the Fourth Amendment. The Ninth Circuit rejected the argument, determining that although the employee had a legitimate expectation of privacy in his workplace office, his employer retained the ability to consent to a search at that office and the employer-owned computer. The employer's IT department had complete access to all employer's computers; the company had a firewall that monitored internet traffic; the company advised employees of its monitoring activities through employee training and an employment manual; and the company told all employees that computers were company-owned and not to be used for activities of a personal nature.

Wasson v. Sonoma County Jr. College Dist.[423]
A terminated community college district employee asserted a 42 U.S.C. section 1983 claim against the district for allegedly invading her privacy by accessing her computer files, in violation of the Fourth and Fourteenth Amendments. The Court determined that the claim lacked merit because a computer policy giving the community college district "the right to access all information stored on district computers" precluded any employee expectation of privacy in the computer files.

United States v. Angevine[424]
The court determined that a University Professor who downloaded, printed and then attempted to delete over 3,000 pornographic images had no legitimate claim for violation of the Fourth Amendment. Not only did University Policy specifically caution employees that information on the network was not confidential and was subject to random audits, but Angevine's own careless attempts at deleting the files showed that he himself did not take sufficient action towards maintaining his own privacy interest.

***Deal v. Spears*[425]**
An owner of a store that had been burglarized installed a recording device to automatically and surreptitiously record all telephone conversations in the hope of identifying whether the criminal activity was an "inside job." The court found that the employer's request to the employee to restrict the frequency of her personal telephone calls and a warning that the calls might be monitored failed to provide sufficient notice that employee telephone conversations would be tape-recorded.

***Biby v. Board of Regents of the University of Nebraska*[426]**
The University terminated Biby, a technology and transfer coordinator, for misrepresenting himself and his authority to a private technology company that later threatened litigation against the University. To investigate the threatened litigation, the University, among other things, searched Biby's work computer files. Biby alleged that the search of his computer violated his constitutional privacy rights. The district court disagreed, granting the University's summary judgment motion, and the Eighth Circuit affirmed. The Court reasoned that public employers may intrude upon constitutionally protected privacy interests of their employees for investigations of work-related misconduct, so long as the searches are reasonable in their scope and manner. The Court found insufficient evidence presented by Biby that the search was unreasonably intrusive. In addition, the Court found that Biby had no expectation of privacy in his workplace computer files because University's policy allowed search of a computer user's files in order to respond to discovery requests.

***Clauson v. Superior Court of Los Angeles*[427]**
The appellate court allowed an employee and his family to pursue both punitive damages for alleged invasion of privacy as well as statutory wiretapping and eavesdropping penalties based on the employee's allegations that his employer installed eavesdropping devices in his office and wiretapped his private office and telephone. Further, the employee alleged that his employer secretly tape-recorded "several hundred telephone conversations" that the employee had with his wife and children and that the taped conversations involved "confidential communications, including private family matters."

McVeigh v. Cohen
The employee in this case was able to successfully argue that his employer had unlawfully monitored his Internet access.[428] Timothy McVeigh, who bears no relation to the Oklahoma City bombing criminal, is a naval officer who sought an injunction to prohibit the Navy from discharging him based on his sexual orientation. The Navy began investigating McVeigh's sexual orientation when a civilian forwarded an e-mail message from McVeigh, sent to her through the America Online Service (AOL), which provided some evidence that McVeigh was homosexual. The Navy then contacted AOL and sought further

information about McVeigh in order to determine his sexual orientation. The court held that the Navy's investigation of McVeigh was illegal under the ECPA since the ECPA only allows the government to obtain information from an online service provider if it (a) obtains a search warrant or (b) if it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question. Accordingly, the court suppressed the evidence since it found that the Navy had unlawfully obtained the information

E. APPLICABLE CALIFORNIA LAW

California employees claiming that the employer breached his/her privacy rights in monitoring his/her electronic communications may potentially assert: (1) violations of Article I, section 1 of the California Constitution which specifically protects privacy, (2) intrusion into seclusion under California Civil Code section 1708.8, and/or (3) the tort of invasion of privacy.

Additionally, California also has two primary bodies of statutory law that specifically governs employer monitoring of electronic communications.

The first is California Penal Code section 502, which was enacted to address the proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.[429] Section 502 protects computer systems, data, the privacy of individuals and "the well-being of financial institutions, business concerns, governmental agencies, and others." It prohibits, in pertinent part, the unauthorized use, copying, damage, interference, and access to lawfully created computer data and computer systems from an internal or external computer or network. The statute provides both criminal and civil remedies. Section 502 explicitly excludes individuals who access their employer's computer systems or data when acting within the scope of their lawful employment. However, the statute does not include similar language protecting the employer from liability. Because the statute only applies to "unauthorized" conduct, the employer may avoid liability under section 502 by obtaining the employee's written acknowledgement and consent to employer monitoring.

In another California Court of Appeal case, *People v. Childs*[430] , the court confirmed the conviction and restitution order of $1.4 million entered against an employee for disrupting or denying computer services to an authorized user (his employer) in violation of Penal Code section 502(c)(5). Penal Code section 502(c)(5) makes it a criminal offense to "knowingly and without permission" disrupt or cause the disruption of computer services or to deny or cause the denial of computer services "to an authorized user of a computer, computer system, or computer network." The employee, Terry Childs, was the principal network engineer for the Department of Telecommunications and Information Services (DTIS) of the City and County of San Francisco. He was assigned to "configure, implement and administer" the City's new fiber-optic wide area network (FiberWAN) using Cisco products. He convinced the City to let him implement the network himself instead of having Cisco do it. Against the expressed concerns of his supervisor, Childs designed the network so that only Childs had access to the passwords to

recover the systems and that, if unauthorized users tried to reboot the system, this would erase the system configurations. Also, in response to the possibility of layoffs in his department, Childs told a coworker, "They can't screw with me, I have the keys to the kingdom."

At some point, the City became concerned about the agitated and potentially violent behavior of Childs. A decision was made to reassign Childs and remove him as the FiberWAN network engineer. When the City met with Childs to reassign him, Childs refused to provide the correct user IDs and passwords for FiberWAN core devices. He first stated that he no longer had administrator access; he then provided incorrect passwords and told the City representatives that he met with that they were not qualified to have the FiberWAN user IDs and passwords. He also refused to provide backup confirmations, stating that there were none.

The City remained locked out of the system from July 9 until July 21, when Childs, through his attorney, gave the correct FiberWan passwords and backup configurations to the Mayor of the City.

After reviewing the legislative history and amendments to Penal Code section 502, the court held that "the Legislature did not intend that subdivision (c)(5) could only be applied to external hackers who obtain unauthorized access to a computer system."[431] Rather, "[i]t appears that subdivision (c)(5) may properly be applied to an employee who uses his or her authorized access to a computer system to disrupt or deny computer services to another lawful user."[432] The court also found that case law supported the application of section 502(c) to employees, "in appropriate circumstances."[433]

Penal Code section 502(c) prohibits knowingly introducing, without permission, a contaminant or lock on a computer, computer system, or computer network for the purpose of restricting an authorized user from accessing the computer, computer system, or computer network.
The second is the California Privacy Act ("CPA")[434] which prohibits the willful attempt to learn the contents or meaning of communications in transit over a wire.[435] As with the federal law, the California Privacy Act only applies to communications during transmission; once an individual receives the communication, the CPA no longer protects it. The consent exception to CPA goes beyond that of federal law because it requires the consent of "all parties to the communication."

The CPA makes it a crime to eavesdrop or record any confidential communication without the consent of all participants to the communication.[436] A confidential communication is any communication carried on in circumstances reasonably indicating that any party thereto desires the communication to be confined to the parties. The prohibition also applies to prevent any of the participants from recording any part of the communication.[437] These sections do not apply to law enforcement agencies in the context of criminal investigations. Also, no person who was not a party to the conversation may disclose the contents of a telegraphic or telephone communication to another person without permission of the person to whom the message was addressed.[438]

In 2017, Penal Code section 632.01 was added, which extended Penal Code section 632 to individuals who "aid and abet" the intentional disclosure or distribution of the contents of a confidential communication with a health care provider that was obtained by that person in

violation of Penal Code section 632. This provision applies to disclosure "in any manner, in any forum, including, but not limited to, Internet Web sites and social media."
In reviewing challenges to an employer's actions in monitoring an employee's electronic communications, California courts determine whether the employee has "a reasonable expectation of privacy" in the electronic communication in question.

> ***TBG Insurance Servs Co. v. Superior Court of Los Angeles County***
> An employer dismissed an employee for violating the company's computer policy by repeatedly accessing pornographic Internet sites while at work. The employee filed a wrongful termination action against the employer. During the litigation, the employee argued that the employer did not have the right to inspect an employer-owned computer the employee had primarily used at home for personal purposes. The employee reasoned that the computer contained significant personal information, including tax information and family correspondence that was subject to his right of privacy under California's constitution. The Court of Appeal ruled in favor of the employer holding that the employee did not have a reasonable expectation of privacy because he consented to the employer's monitoring of his computer activities by signing the employer's computer use policy.[439]

Employers should be aware of Labor Code section 980, effective January 1, 2013, which prohibits employers from requiring or requesting that an employee or applicant:

- Disclose a username or password for the purpose of accessing personal social media;
- Access personal social media in the presence of the employer; or
- Divulge any personal social media.

Labor Code section 980 defines "social media" as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."[440] Section 980 does not affect an employer's "existing rights and obligations" to request an employee to divulge personal social media when "reasonably believed" to be relevant to an investigation into employee misconduct. Thus, to the extent an employer already has a right to request an employee to divulge personal social media as part of an investigation into employee misconduct (e.g., the alleged acts have a nexus to the employee's employment and the employee's right to privacy is outweighed by the employer's interest in preventing and addressing the alleged misconduct), section 980 does not affect the employer's ability to request this information. Also, an employer is not precluded from asking an employee for a username or password to access employer-issued electronic equipment.

Other California statutes prohibit the intentional recording of a confidential communication "by means of any electronic amplifying or recording device" without the consent of all parties.[441] For example, California Penal Code sections 631-633 generally prohibit the eavesdropping and

recording or intercepting of certain communications. Certain law enforcement officers are exempt from these provisions. In addition, these exemptions have been extended to POST-certified police chiefs, assistance police chief or police officers of a university or college campus who are acting within the scope of their authority and provided they overhear and record communications, within certain parameters, during a criminal investigation related to sexual assault or another sexual offense.

Telish v. California State Personnel Bd.[442]

This case involved a Senior Special Agent in Charge at the Bureau of Narcotics Enforcement's L.A. Interagency Metropolitan Police Apprehension Task Force ("LA IMPACT") who threatened to post on-line sexually explicit photographs that he had taken of an employee that he supervised unless she recanted her statements about a consensual sexual relationship that she had with him. When the employee eventually reported the threat and another incident to her boss, the boss reported the incidents to the DOJ and solicited the assistance of the employee in recording the statements of the senior agent about their relationship. The court determined that the recordings did not violate Penal Code section 632, even though they were done without the consent and knowledge of one of the senior agent, because they were done at the direction of law enforcement as part of a criminal investigation. The evidence was then used as part of an administrative proceeding to terminate the senior agent. The court permitted the evidence to be used in the administrative proceeding because it had been obtained lawfully for the criminal investigation and nothing in the statute restricted how the information could be used once it was lawfully obtained.

F. CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT – APPLICATION TO PUBLIC EMPLOYER'S ABILITY TO SEARCH EMPLOYER OWNED ELECTRONIC DEVICES AND EMAILS

California's Electronic Communications Privacy Act, codified under Penal Code section 1546, et. seq., generally limits a government entity from searching or accessing information on an electronic device (e.g., smartphone, computer) or electronic information on a network (e.g., email) without a search warrant or court order.

Under the Penal Code a government entity shall not do any of the following:

- Compel the production of or access to electronic communication information from a service provider.
- Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
- Access electronic device information by means of physical interaction or electronic communication with the electronic device.[443]

The legislative intent of the law, and subsequent case law, appears to be aimed at law enforcement agencies conducting criminal investigations. The use of the terms "law enforcement" and "police" supports this conclusion.

While this law was generally intended to address privacy concerns around law enforcement searches of electronic devices and communications, if it is determined by courts to broadly apply to government entities it may negatively affect the ability to conduct such searches of an employee's electronic devices or communications.

The statute generally protects an "authorized possessor" of electronic devices, defined as "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device." (Pen. Code, § 1546(b).) (emphasis added). A government entity may only access electronic information "with the specific consent of the authorized possessor of the device." (Pen. Code, §§ 1546.1(c)(3).) (emphasis added).

We do not believe that section 1546.1 would be interpreted to allow a public employee who has been provided an electronic device owned by the government entity to exert the rights of an "authorized possessor" under this law and decline a search by the government entity that actually owns the electronic device. Nonetheless, this ambiguity in the law does highlight the importance for public agencies to clarify in their electronic use policies that an employee's use of an electronic device owned by the government agency is subject to search and the obligation to surrender the electronic device at any time by the public agency.

The Penal Code does not state that a government entity is prohibited from searching for electronic information on its own network or email system. Rather, the statute provides that a search to "compel the production of or access to electronic communication information from a service provider" can only occur with a warrant or court order. Therefore, the statutory language does not appear to apply to searches of an internal network or email system maintained by the government entity itself. Interpreting the statute's restrictions otherwise would mean that a government entity that maintains its own network and email system needs a warrant or court order to search its own network and email system. We do not believe that is reasonable, nor what the Legislature intended through the passage of SB 178.

Importantly, the statutory language does limit a government entity from searching an employee's personal electronic device and personal electronic information maintained by a service provider (e.g., personal email account such as Gmail or Yahoo). This is because when it comes to such electronic devices, the government entity is not the owner or the "authorized possessor" of the device. In the case of an employee's personally owned cell phone, the employee is the owner and/or "authorized possessor" of the cell phone and would either have to give permission to a government entity to search the device or the government entity would have to get a search warrant/court order to conduct such a search of the device.

The same result would also most likely apply for searches of other electronic information provided by an outside service provider. To the extent that a government entity does not directly control an employee's electronic information that is being sought, the government entity would need to get permission from the employee to search it or otherwise get a warrant or court order to compel a third party service provider to disclose such information.

LCW Practice Advisor

Here are a few best practices public employers can follow:

Review and revise electronic communications policies to limit an employee's expectations of privacy in the use of government-owned electronic devices and the use of work email maintained by the governmental entity;

Reinforce that a public employee's authorization to use a government-owned electronic device is at the sole discretion of the government entity and can be modified or revoked at any time, that such electronic devices are subject to search, and an employee is obligated to surrender the electronic device back to the government entity at any time; and

Seek legal counsel before compelling a public employee to allow a search of their personally owned electronic devices or of personal electronic information that is maintained by an outside service provider and not directly controlled by the government entity.

G. GUIDELINES FOR ELECTRONIC COMMUNICATIONS IN THE WORKPLACE

Employers have legitimate reasons for ensuring that their electronic communications systems are not abused by employees. In California, courts would likely find that an employee does not have a reasonable expectation of privacy when he or she has given written consent to monitoring of the employer's computers and electronic system.[444] For this reason, employers must have a written Electronic Communications Resources Policy that puts employees on notice of the following:

- Electronic communications such as voicemail, e-mail and/or systems accessible via the Internet are the employer's property and should only be used for legitimate business purposes during working hours. This prohibition is not meant to interfere with an employee's right to organize or discuss the terms and conditions of his/her employment with others during nonworking hours through the use of employer email systems.

- ❑ The employer reserves the right to monitor any of its electronic communications systems (including voicemail, e-mail, and the Internet) to assure that its property is being used for business purposes only during working hours and to prevent any unlawful or improper use.
- ❑ Employees do not have a personal privacy right in any matter created, received, stored in or sent to an electronic system, maintained by the employer.

It is important to note that an NLRB decision recognized the right of employees to engage in Section 7 activities during non-working hours through the use of an employer's email system unless special circumstances justify a business use only restriction.[445] Special circumstances in support of a total ban on non-business emails during non-working hours require a showing that the restriction is necessary to maintain production or discipline.[446] An employer may also institute controls on the use of non-business emails during non-working hours when the controls are applied uniformly and consistently enforced to the extent they are necessary to maintain production and discipline.[447]

1. "ATTORNEY-CLIENT COMMUNICATIONS" SENT THROUGH WORK E-MAIL

In a decision entitled *Holmes v. Petrovich Development Company*[448], the California Court of Appeal in Sacramento held that e-mails sent by an employee to her attorney regarding possible legal action against her employer did not constitute confidential attorney client communications because the employee used the employer's computer even though (1) she had notice of the employer's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal e-mail, (2) she had notice that the company would monitor its computers for compliance with the employer's policy, and (3) she had been explicitly advised that employees using company computers to create or maintain personal information or messages "have no right of privacy with respect to that information or message." The employer was thus entitled to introduce the emails as exhibits in the employee's trial of her discrimination and harassment lawsuit against the employer.

Holmes worked for Petrovich Development as the Executive Assistant to Paul Petrovich, the Company principal. One month after her hire she advised Petrovich that she was pregnant. A series of exchanges between Petrovich and Holmes took place over the next several weeks until she resigned and subsequently claimed that she had been constructively discharged. Eventually she sued the company alleging sexual harassment, retaliation, wrongful termination, violation of public policy, violation of the right to privacy and intentional infliction of emotional distress. The company obtained summary adjudication on three of Holmes' claims and obtained a jury verdict in its favor on the remaining claims which went to trial.

Prior to Holmes' resignation she had exchanged emails with her attorney seeking advice on her rights, specifically related to pregnancy discrimination. She used the company computer and email system. The company later accessed and read these emails and actually used some of them as exhibits in the subsequent jury trial. Holmes attempted to prevent the introduction of the emails into evidence and sought a court order demanding the return of the emails as privileged

documents. She also challenged about a limiting instruction given to the jury by the trial judge which she claimed undermined her claim of invasion of privacy.
The Court of Appeal rejected all of Holmes' claims and affirmed the trial court judgment.

The Court of Appeal concluded that by using the company computer and email system to send and receive emails with her attorney, Holmes lost the attorney-client privilege and any reasonable expectation of privacy. The Court explained that an attorney-client communication does not lose its privileged character solely because it is electronically communicated. However, "the e-mails sent via company computer under the circumstances of [the Holmes] case were akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him".

Holmes once again points to the need for employers to have comprehensive written and promulgated policies spelling out the terms and conditions of employee use of company computers and making it clear to employees that they have no expectation of privacy in anything they send or receive on company computers.

2. OTHER TYPES OF "PRIVILEGED" COMMUNICATIONS SENT THROUGH WORK E-MAIL

Several cases in jurisdictions outside of California have examined whether other types of privileges attach to communications sent on work computers.

> ***In re the Reserve Fund Securities and Derivative Litigation*[449]**
> A district court in New York looked at whether the marital privilege protected e-mail communications sent by an employee to his spouse through his employer's e-mail system. The court held that the privilege did not apply and the communications were discoverable because the employee did not have a reasonable expectation of privacy in the communications.
>
> Although communications between spouses are presumed to be confidential, this presumption will be lost if the communication, "because of its nature or the circumstances under which it was made, was obviously not intended to be confidential."[450] The court looked at whether the employee had a "reasonable expectation of privacy" in the e-mail communications made to his wife. If a reasonable expectation of privacy did not exist, the spouses could not have intended for the communications to be confidential and the marital privilege would not apply.
>
> In determining whether a "reasonable expectation of privacy" existed in e-mails transmitted through his employer's e-mail system, the court applied the four-factor test in *In re Asia Global Crossing, Ltd.*[451], which is:

1. does the corporation maintain a policy banning personal or other objectional use,
2. does the company monitor the use of the employee's computer or e-mail,
3. do third parties have a right of access to the computer or e-mails, and
4. did the corporation notify the employee, or was the employee aware, of the use and monitoring pieces?[452]

The answer to these questions is "highly fact-specific" and are "largely determined by the particular policy language adopted by the employer."[453] In applying this test to the facts in *In re the Reserve Fund Securities and Derivative Litigation*, the court found that: (1) the employer had an e-mail policy that clearly banned personal use the employer's email system, (2) while the policy stated that the employer will not "routinely monitor e-mail and will take reasonable precautions to protect the privacy of e-mail," it also "reserve[d] the right to access an employee's e-mail for a legitimate business reason . . . or in conjunction with an approved investigation"; (3) the policy specifically warned employees that their e-mail communications would be "automatically saved" and are subject to review by the employer and by disclosure to third parties, and (4) the employee admitted he was aware of the employer's policy. Thus, the court found that the employee had no reasonable expectation of privacy in the e-mails and that the marital privilege did not apply.[454]

H. VIDEO SURVEILLANCE OF EMPLOYEES

Situations may arise, such as suspected theft or other misconduct, where an employer finds it wants to conduct hidden video surveillance of its employees. However, employers have to balance their desire to conduct hidden surveillance against the employees' right to privacy.

Note: *Labor Code Section 435 prohibits an employer from making any audio or video recording of an employee in a restroom, locker room, or other room designated for changing clothes, unless authorized by a court order.*

Hernandez v. Hillsides, Inc. [455]

The California Supreme Court addressed an employee's right to privacy in the workplace following an employer's use of a hidden video surveillance camera in an enclosed office as part of an investigation into possible employee misconduct. In *Hernandez*, the employer operated a residential facility for abused children. The executive director installed a hidden video camera into an enclosed office shared by two employees after learning that someone was accessing pornography sites from one of the computers after hours. The camera was only operational a few nights after regular working hours and neither of the employees was captured on film.

The Court concluded that Hillsides was not liable for an invasion of privacy. This case was somewhat unique because Hillsides had an acute interest in preventing individuals from viewing pornography in light of the organization's goal to provide a wholesome environment for the abused children in its care.

The Court pointed out that employers should generally not use such video surveillance in the workplace without providing "adequate notice to persons within camera ranges that their actions may be viewed and taped." While the Court's decision does not necessarily mean that employers must provide details of video surveillance methods used in the workplace, an employee should be placed on express notice that such methods may be used. Unlike other notice provisions that are often contained in an Employee Handbook, there is a strong inference from this decision that employers should provide a separate notice and acknowledgment form to employees that video surveillance may be used in the workplace. Employees should require that employees review and sign the separate acknowledgment form to indicate that they are on notice of the potential for video surveillance in the workplace

Sacramento County Deputy Sheriff's Association v. Sacramento County et al.
The court held that deputy sheriffs working in a jail environment have diminished privacy expectations because of the nature of their employment.[456] In that case, prison officials were investigating the apparent theft of inmates' cash from the office. Based on those circumstances, the court found that the deputies did not have a reasonable expectation of privacy against being videotaped by hidden cameras in that office. Therefore, warrantless, video-only surveillance did not constitute unlawful search and seizure, invasion of privacy, or tortuous intrusion into deputies' privacy.

Trujillo v. City of Ontario
The United States District Court for the Central District of California found that an employer violated police officers' federal and state rights to privacy by conducting videotape surveillance of a locker room in order to investigate theft of a flashlight. The conduct in question took place before the enactment of California Labor Code section 435, which expressly prohibits videotaping of employee restrooms, locker rooms, and changing areas. The *Trujillo* case balances the need to investigate theft against employee privacy interests, and provides a detailed evaluation of the elements by which to analyze public employee invasion of privacy claims.[457]

Trujillo can be read as supporting a right to monetary damages for violation of the California constitutional right to privacy. However, subsequent to *Trujillo*, the district court for the Eastern District of California ruled in *Blanco v. County of Kings*[458] that *Trujillo* assumed, without deciding, that money damages are available for a California constitutional right to privacy claim. The district court

for the Eastern District of California held that "in the absence of affirmative authority that clearly establishes a right to monetary damages under the California constitutional right to privacy, . . ., [it] declines to permit a cause of action for damages under the California Constitutional right to privacy."[459]

Richardson-Tunnell v. School Insurance Program for Employees (SIPE) [460]
A public agency and its employees are immune from liability for conducting video surveillance as part of judicial and administrative proceedings, such as a worker's compensation case. In *Richardson-Tunnell v. School Insurance Program for Employees (SIPE),* the Second District Court of Appeal held that a public entity is immune from liability for its covert videotaping of wedding and honeymoon of employee who was off work due to alleged employment related injury. The employee injured her back at work and filed a worker's compensation claim in June 2003. During her disability leave, she got married. The District and its workers' compensation insurer hired an investigator to surreptitiously attend the employee's wedding to videotape her. The investigator misrepresented himself as an invited guest and videotaped the employee at her wedding and during her honeymoon.

The employee filed suit against the investigator, the District, and worker's compensation insurer alleging, among other things, violations of her constitutional rights to privacy and of Civil Code section 1708.8. The Court of Appeal held that under Government Code section 821.6, public employees are granted immunity for instituting or prosecuting judicial or administrative proceeding within the scope of their employment, even if their conduct is malicious and without probable cause. The investigation was initiated during the worker's compensation case and was therefore part of judicial and administrative proceedings subject to section 821.6 immunity.

Sanders v. American Broadcasting Companies, Inc. [461]
The California Supreme Court upheld a damage award against ABC news after one of its reporters went undercover as an employee and videotaped private conversations between co-workers. The video was later shown on ABC and an employee sued. The Court held that the employee had an expectation that his comments would not be made public, even though the comments were made in a setting in which other employees could hear the comments.

Ops.Cal. Atty Gen No. 12-110 [462]
The California Attorney General has issued an opinion that continuous videotaping surveillance of commercial drivers did not constitute a misdemeanor under Labor Code section 1051, when the video file is inspected by a third party who is an agent of the driver's employer and the videotape surveillance is for the sole benefit of the driver's employer.

The manner of surveillance and the area under surveillance may also play a role in determining whether a privacy interest is invoked in the workplace. As a result, employers are advised to consult with legal counsel to review their video surveillance procedures and policies in the workplace.

LCW Practice Advisor

Education Code Section 78907 prohibits the use by any person, including a student, of any electronic listening or recording device in any classroom without the prior consent of the instructor. The only exception is to provide accommodation to disabled students.

In addition, an educational institution cannot simply install security cameras without providing notice and an opportunity for the relevant employee associations to bargain and negotiate the effects of a decision to install security cameras.[463] This is the case regardless as to whether the cameras are overt or covert and whether the cameras are install in public or private portions of the premises.[464]

While there are limitations on what recording an employer can do at the workplace, there are also limitations on what types of recordings an employer can prohibit of employees in a workplace. In the National Labor Relations Board ("NLRB") decision *Whole Foods Market, Inc.*[465], the Board prohibited a private employer from having a "no-recording" rule that prohibited employees audio and/or video recordings in company meetings without prior approval and also prohibited recording conversations with a tape recorder or other recording device unless the employee received prior approval from store or facility leadership. The Board found that the rules, while not expressly prohibiting employees from engaging in protected activities, could be reasonably construed by employees to prohibit concerted protected activity. This is because there are many situations where an audio and/or video recording may used to promote mutual aid or protection such as recording picketing, documenting unsafe workplace equipment, or documenting the inconsistent application of workplace rules. Therefore, the rules were required to be rescinding.

While the NLRB decision is not binding on California public agencies, PERB often uses decisions issued by the NLRB when interpreting issues arising in the public sector and thus it is important to be aware of how the NLRB is interpreting these issues.

I. TRACKING DEVICES

Various tracking devices have entered the market: Radio Frequency Identification (RFID), Global Positioning Systems (GPS), and Event Data Recorders (EDR). These devices are available to private individuals for their personal use. For example, cellular telephone companies are now providing GPS as part of their services. However, employers should proceed with caution in using these technologies.

Generally, individuals in California are prohibited under Penal Code section 637.3 from using electronic tracking devices to determine the location or movement of a person.[466] An exception exists that allows registered owners, lessors, or lessees of vehicles to use electronic tracking devices to track their vehicles.[467] In other words, if the agency owns or leases a vehicle, that agency may use GPS, or similar electronic tracking devices, to monitor the location or movement of its employees. An exception also applies to the lawful use of a tracking device by a law enforcement agency.[468] In *United States v. Jones*, the United States Supreme Court held that the government's use of a GPS device, without a warrant, during a criminal investigation, to monitor a vehicles movement violated the Fourth Amendment to the U.S. Constitution[469]

"Telematics" refers to sending, storing and receiving information through telecommunication devices.[470] Telematics once meant the merging of computers and telecommunications.[471] Today, the term "telematics" more commonly refers to automation in automobiles, including integrated hands-free cell phones, GPS navigation, wireless communications, and automated driving assistance systems, including General Motor's OnStar system.[472]

Vehicle telematics may be used to track and monitor a vehicle or a fleet of vehicles, recover stolen vehicles, provide automatic collision notification and provide in-vehicle early warning prevention alerts.[473] Additionally, built-in vehicle telematics systems can be used to identify electronic or vehicle maintenance problems and provide information to the manufacturer and owner.[474]

While a public agency is allowed to track the use of vehicles it owns or leases, it should implement this technology only where it has a legitimate business reason for doing so, and in a manner that puts employees on notice that they will be monitored. This should help the public agency avoid any arguments by employees that it is violating their privacy rights. Public agency employers should implement written policies that inform employees that their use of the agency vehicle will be monitored. The written policy should also discuss some of the business reasons for monitoring employees, such as measuring productivity, locating stolen vehicles, providing aid to vehicles that break down, or ensuring that employees are following their routes or assignments.

Disciplinary actions by employers that have a "significant effect on the wages, hours and other terms of the conditions of employment" are subject to the mandatory bargaining requirements of the Meyers-Milias-Brown Act.[475] Therefore, employee discipline would likely be subject to mandatory bargaining to the extent it results from information obtained via tracking technology on agency-owned or leased vehicles, including discipline for misuse of the equipment, inappropriate use of time, and speeding.[476]

While GPS tracking is now widely available through cellular telephones, employers should not use it. The Penal Code prohibits such tracking,

> *"No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person."*[477]

In addition to a violation of the Penal Code, employee tracking with the use of cellular telephones or similar devices may raise employee privacy claims under the California and United States Constitutions.

J. BIOMETRICS

"Biometrics" is an automated method used to recognize an employee's unique physiological or behavioral characteristics.[478] *Biometrics is a general term that is used to describe a process or a characteristic.*[479] Biometrics is often used to improve security and productivity in the workplace. "Physiological biometrics" include fingerprint scanners or sensors, and iris recognition technology.[480] "Behavioral biometrics" include voice, keystroke, gait and signature recognition capabilities.[481] Biometrics is used to track productivity and to grant employees access to secured workspaces or locations.

Biometrics pose privacy considerations for employers because it requires that employers collect employee physiological or behavioral data. The collection and storage of this highly confidential information poses both privacy and security risks for employers. Generally, this data is electronically stored. Employers must weigh the risk of privacy violations that will result if an employee's personal data is lost, stolen or misplaced against the convenience that using biometrics may afford to employers. For example, because fingerprints are unique to each person, the risk of identity theft is great if a hacker were to obtain fingerprint information along with other employee data. Because of the risks involved with the use of this technology, employers should use biometrics only when they have legitimate business needs that justify its use. For example, employers may use biometrics to restrict access to highly secured buildings, such as prisons. However, we advise that all employers seek legal counsel and technical advice before implementing this type of technology.

K. EMPLOYER'S AFFIRMATIVE DUTY TO REPORT EMPLOYEES' UNLAWFUL ACTIVITY ON THE INTERNET

In a case of first impression, an appellate court in New Jersey has found that, under certain circumstances, an employer may be subject to a common law negligence claim for failing to report an employee's use of workplace computers to access child pornography. In *Doe v. XYC Corp*[482], a mother brought an action for negligence on behalf of her minor daughter against her husband's employer for failing to report the husband's use of a workplace computer to access pornography and send nude photos of the daughter to a child porn site. The trial court granted the employer summary judgment on the grounds that it had no duty. The appellate court reversed finding that the employer's computer use policy, which included monitoring employee's computer use and resulted in the detection of employee's access to child porn sites, created a duty to report the "employee's activities to the proper authorities to take effective internal action to stop these activities whether by termination or some less drastic remedy." This case does not reflect California law, and it is unclear if it reflects current trends in the law. The decision is instructive, however, in that it raises questions concerning whether an employer has

an obligation to report an employee engaging in illegal conduct on the Internet to the authorities once that misconduct is discovered via monitoring.

SECTION 7 REGULATION OF PERSONAL AND OFF-DUTY CONDUCT

Employers are only permitted to control off-duty conduct or relationships in limited circumstances. The touchstone in all of these is job nexus, or connection to the position in question. This section will explore the laws that define and limit the circumstances in which an employer can control, interfere with, or base employment decisions upon, off-duty conduct or relationships.

Legal snapshot: Personal and Off-Duty Conduct	
Applicable laws:	• Constitutional Right of Privacy (Cal. Const. art. I, § 1) • First and Fourth Amendment of the U.S. Constitution • Title VII of the Civil Rights Act of 1964 • Fair Employment and Housing Act (FEHA), Cal. 3 (Gov. Code § 12900 et seq.) • Public Safety Officers' Procedural Bill of Rights Act, Cal. Gov. Code §§ 3300 *et seq.* • Various other federal and California statutes • Common law torts
Who and what is protected?	• Applicants and employees • Personal workplace relationships • Personal activities and off-duty conduct
Generally, employers must NOT:	• Base hiring and promotional decisions on personal relationship unless it would pose an unreasonable workplace conflict or hazard • Base employment decisions upon employees' personal conduct unless there is a sufficient nexus to the employee's position

The balancing test for this is:	• Employee's right of privacy in personal relationships and activities versus employer's legitimate workplace interests of productivity and safety

A. WORKPLACE RELATIONSHIPS

1. MARITAL STATUS AND ANTI-NEPOTISM POLICIES

Federal and state equal employment opportunity laws, as well as the state Constitution, generally prohibit employers from making employment decisions based upon an employee's marital status.

However, anti-nepotism policies are permissible under narrow circumstances, when the marital status creates an unreasonable workplace conflict or hazard, and when the policies are narrowly tailored to respond only to the conflict or hazard.[483]

Once it is determined that a legally recognized conflict-of-interest problem exists because of the relationship, explore all options, and take action that is non-discriminatory.

- Consider reassignment or transfer options.
- Consult affected individuals.

Make the reassignment, transfer or termination action based on preferences of employees involved, or, if none, then on objective standards (personnel rules, memorandum of understanding, other relevant statutes, rules or regulations, past practice, seniority).

Marital Status Provides Unfair Commission Advantage
The DFEH upheld an insurance company employer's denial of a position to the spouse of one of its salespeople. This was based upon a concern that spouses might pool sales by reporting the sale under one of the spouse's names to increase commissions.[484]

Marital Status Creates Access to Personnel Information
The DFEH upheld a city employer's denial of a mechanic's position to the husband of one of its employees. This was based upon the concern that his wife was a clerical worker in the department to which he applied, and the wife might reveal to her husband confidential information contained in the personnel files and time records to which the wife had access.[485]

2. CHECKLIST: GUIDELINES FOR ANTI-NEPOTISM POLICIES

- ❑ Review and update any current nepotism policy to make sure that it complies with the law prohibiting marital status discrimination.
- ❑ Individually review any facts regarding a potential problem with supervision, safety, security or morale.
- ❑ Supervision - is it likely that one of the spouses or related individuals would have supervisory responsibilities over the other?
- ❑ Safety - is it possible that one of the spouses or related individuals may be responsible for making an important or emergency decision or taking any action that could be affected by the spouse or related individual's co-employment?
- ❑ Security - does the relationship raise questions about an individual's ability to maintain the confidentiality or security of the employer's property or matters to which the employer has a duty of confidentiality?
- ❑ Morale - would or does the relationship pose problems for morale? Normally this would arise in connection with problems with supervision, safety or security.

3. CONSENSUAL WORKPLACE ROMANCES AND SEXUAL FAVORITISM

Similar problems with supervision, safety, security or morale may exist when co-workers have special off-duty relationships. For example, dating among co-workers is common. Occasionally, co-workers will develop long-term relationships and perhaps live together. Employees have a strong expectation of privacy in these personal, off-duty relationships. However, an employer has a legitimate interest in controlling or preventing any adverse effects the relationship has on supervision, safety, security or morale.

A supervisor's consensual sexual relationship with a subordinate does not per se violate federal or state anti-discrimination laws or public policy. Similarly, preferential treatment by a supervisor towards his/her paramour does not, by itself, constitute sex discrimination in violation of the Fair Employment and Housing Act (FEHA) or Title VII.[486]

In the 2005 landmark decision of *Miller v. Department of Corrections*[487] the California Supreme Court definitively recognized that an employee may establish an actionable claim of sexual harassment under the FEHA by demonstrating widespread sexual favoritism that was severe or pervasive enough to alter his or her working conditions and create a hostile work environment. In short, the California Supreme Court added sexual favoritism to the list of conduct that can constitute sexual harassment.

***Proksel v. Gattis*[488]**

In *Proksel*, a male supervisor showed preferential treatment toward a female word processor with whom he was allegedly having an affair by giving her a larger year-end bonus than any other employee, more valuable Christmas gifts, and going with her to a private birthday lunch. Even so, the court held that the supervisor's preferential treatment toward an employee with whom he is romantically involved is not—in itself—sex discrimination under FEHA.

The *Proksel* case relied, in part, on a policy statement put out by the Equal Employment Opportunity Commission (EEOC) in 1990:

Not all types of sexual favoritism violate Title VII. It is the Commission's position that Title VII does not prohibit isolated instances of preferential treatment based on consensual romantic relationships.

Even when no sexual favoritism exists in a consensual supervisor-subordinate relationships, such relationships can result in other forms of serious liability exposure. There are numerous cases involving claims of harassment brought by the paramour employees themselves, after their consensual relationships with a supervisor ended.

For example, in *Samson v. Allstate Insurance Co*., an attorney had a consensual romantic relationship with his legal secretary for two years, after which the secretary ended the relationship.[489] After the secretary left the job, she filed a claim against her employer alleging sexual harassment (that her employer made advances to her within the first weeks of her employment and she acquiesced and continued in the relationship out of fear of losing her job) and retaliation (that after she ended the relationship, her employer changed the terms of her employment). Clearly, the potential exists for consensual romantic relationships between supervisors and subordinates to later form the basis for harassment claims.

The upshot of these sexual harassment cases is that employers have a very strong interest in learning of and regulating workplace romantic relationships to insure no unlawful harassment develops. As the above cases demonstrate, romantic relationships in the workplace can result in harassment claims by one of the persons in the relationship or by coworkers affected by it. This strong employer interest exists notwithstanding employee claims that they have privacy interests in such relationships.

As with other aspects of privacy law, neither the Courts nor the Legislature have delineated "bright line" standards to guide employers in this area. In general, a Court will more likely find an employer's investigation and response to a workplace relationship legitimate if the employer's conduct has a strong relationship to the detection and prevention of harassment and if it is narrowly tailored to avoid unnecessary intrusions into private matters.

It is more likely that employers will have protection from privacy claims when one party to the relationship complains to management. In that circumstance, an employer's anti-harassment policy should mandate an investigation or other response. A Court will likely find that the employer's interests in responding to a harassment claim will supersede privacy interests. Federal (not California law when the alleged harasser is a supervisor) law allows an employer to avoid vicarious liability if the employer proves, among other things, that it "exercised reasonable care to prevent and correct promptly any sexually harassing behavior . . . ."[490]

4. ANTI-FRATERNIZATION POLICIES

Policies prohibiting "fraternization" or dating between supervisory employees and their subordinates are not unconstitutional or illegal per se, and employers may be able to demonstrate legitimate business reasons for prohibiting dating or sexual relationships between supervisory employees and their subordinates. However, it would likely be more difficult for an employer to prove that it had a legitimate business interest in prohibiting relationships between employees of equal status than between supervisory/subordinate employees.

Barbee v. Household Automotive Finance Corp.
A California appellate court upheld a "conflict of interest" policy, that stated in part, that a supervisor involved in a consensual intimate relationship with an employee within that supervisor's direct or indirect area of responsibility, must bring the relationship to management's attention for appropriate action, including reassignment to avoid a conflict of interest.[491] A supervisory employee who had been given a choice of either terminating a romantic relation with a subordinate or resigning, challenged the policy. The California Court of Appeal upheld the policy. The court found that even assuming the supervisor had a legally protected privacy interest in his intimate relationship with a subordinate, he could not establish that he had a reasonable expectation of privacy in such a relationship.[492]

The *Barbee* court noted that employers have legitimate interests in "avoiding conflicts of interest between work-related and family-related obligations; reducing favoritism or even the appearance of favoritism; [and] preventing family conflicts from affecting the workplace." The court further noted that managerial-subordinate relationships present issues of potential sexual harassment.

Crosier v. United Parcel Service, Inc.
The employer, UPS, had an unwritten rule prohibiting social relationships between management and non-management employees.[493] The plaintiff, a management employee, claimed wrongful termination on the grounds that his dismissal for violation of this non-fraternization rule was not for good cause. In determining whether his dismissal based on this violation constituted good cause, the court reasoned that it must balance the employer's interest in operating his business efficiently and profitably with the interest of the

employee in maintaining his employment. The court found that the employer was legitimately concerned with appearances of favoritism, possible claims of sexual harassment and employee dissension created by romantic relationships between management and non-management employees.

Employers should consider the following in reviewing their policies:

- Does your agency's interest in preventing workplace problems due to these types of relationships justify the invasion of employees' privacy?
- How would your agency determine whether employees were violating the policy?
- How would your agency ensure that the policy is being enforced uniformly?

5. INVESTIGATION OF WORKPLACE ROMANCES AND SEXUAL FAVORITISM

An employer's investigation and regulation of its employees' workplace, sexual and dating relationships triggers employee privacy rights. The following cases provide some guidance on the contours of these rights. Although the cases are from more than twenty years ago, they remain good law. They also illustrate the continued theme of regulating workplace romances – whether regulation and investigation is legitimate turns on the extent to whether the activity in question has a job performance or other workplace nexus.

Shuman v. City of Philadelphia
The City dismissed a police officer for refusing to answer investigative questions pertaining to his private sexual activities with a woman who was not a member of the employing agency. The officer alleged the dismissal violated his privacy. The Court agreed, holding that absent a showing that a police officer's off-duty personal activities had an impact upon his or her job performance, the City's inquiry into the officer's private sexual conduct violated the officer's constitutionally protected privacy rights.[494]

Thorne v. City of El Segundo
A female clerk typist in the police force applied for a police officer position, but the City denied the application, in part, based on a polygraph test session in which the employee admitted she had suffered a miscarriage and that the father of the child was an officer on the police force. The applicant sued for invasion of privacy among other things. The Ninth Circuit upheld the claim. It emphasized that an employer's intrusion into an employee's private sexual activity must have a workplace nexus to be legitimate. "In the absence of any showing that private, off-duty, personal activities of the type protected by the constitutional guarantees of privacy and free association have an impact upon an applicant's on-the-job performance, and of specific policies with narrow implementing regulations, we hold that reliance on these private non-job-related considerations by the state in rejecting an applicant for employment violates the

applicant's protected constitutional interests and cannot be upheld under any level of scrutiny."[495]

Shawgo v. Spradlin
A City disciplined male and female police officers for off-duty dating and alleged cohabitation in violation of applicable department regulations. The Chief of Police defended the regulations on the ground that they proscribed conduct which "if brought to the attention of the public, could result in justified unfavorable criticism of that member of the department." The Fifth Circuit found no infringement of the employees' privacy rights. It reasoned: "We agree with the district court that, in the present circumstances, the plaintiffs' right to privacy has not been infringed by the scope of the regulation proscribing, as conduct prejudicial to good order, cohabitation of two police officers, or proscribing a superior officer from sharing an apartment with one of lower rank."[496]

B. OFF-DUTY CONDUCT

1. APPLICABLE LEGAL STANDARDS

a. Bases for Regulating Off-Duty Conduct – "Nexus to Employment"

The United States and California Constitutions protect the privacy of employees in their off-duty conduct. Employers must not unreasonably regulate/restrict that conduct, and must not base employment decisions on off-duty conduct that does not have a relationship to the employment. The Ninth Circuit Court of Appeals, in *Thorne v. City of El Segundo*,[497] stated the rule as follows:

> *"In the absence of any showing that private, off-duty, personal activities of the type protected by the constitutional guarantees of privacy and free association have an impact upon an applicant's on-the-job performance, and of specific policies with narrow implementing regulations, we hold that reliance on…private non-job-related considerations…in rejecting [or making any employment decision regarding] an applicant for employment [or employee] violates the [individual's] protected constitutional interests."*

The necessary relationship is usually referred to as "job nexus." Nexus is determined not only by the type of off-duty conduct but by reference to the type of employer and duties and responsibilities of the particular position in question. Courts have also found a nexus where an employee's off-duty conduct creates a conflict of interest or where an employee's illegal off-duty conduct undermines an employee's or agency department's credibility with the public.

For example, an employer does not have a legitimate interest in knowing about a police officer applicant's prior sexual associations, sexual practices, and miscarriage. The employer would have to show that its inquiry was justified by a legitimate compelling interest of the department, that the inquiry was narrowly tailored to meet those legitimate interests, and that the department's use of the information was proper and in furtherance of the legitimate compelling interest.

Anderson v. State Personnel Board
A police department was justified in terminating a highway patrol officer for intentionally appearing nude in sight of neighborhood women and children on numerous occasions over a period of time. The officer lost his credibility with allied law enforcement agencies and his peers, and brought embarrassment to the department.[498]

Fleisher v. City of Signal Hill
A police department also lawfully terminated an officer who had engaged in sexual conduct with a minor explorer scout while they were both explorer scouts in the department. The department had an interest in ensuring that minor girls who join the explorer program did not become the victims of statutory rape as a result of their participation in the program. The department also had an interest in protecting injury to its reputation and the morale of the department.[499]

Fugate v. Pheonix Civil Service Board
A police department was justified in terminating vice officers for having sexual relations with prostitutes. The department demonstrated that the off-duty conduct created conflicts of interest and a possibility of blackmail. Further, it undermined the department's internal morale and community reputation.[500]

A police officer's continuing association with a convicted felon in violation of department rules has also satisfied the grounds for lawful termination. *In Bailey v. City of National City*, the officer had been warned to cease his contacts with a close friend, to no avail. The court supported the termination decisions on the basis that associating with a felon could bring disrepute upon an officer by tempting him not to impartially perform his duties, or by conveying the impression that law enforcement might not be even-handed. The officer's disregard of departmental rules and direct orders was also a factor considered by the court, as they were viewed as undermining the command structure's reliance on obedience to rules and directives.[501]

Employers should keep in mind that courts recognize a significant difference between job-relatedness of off-duty conduct in the case of law enforcement employees and non-safety employees.

There is generally no nexus between an employee's private, off-duty use of illegal drugs or alcohol as long as it does not involve on-the-job impairment. In

Vielehr v. State Personnel Board,[502] the court considered the issue of whether a state tax representative trainee with the Department of Human Resources was properly dismissed for his conviction of possession of marijuana while off-duty. The court reversed and remanded the case to the trial court on the grounds that no obvious relationship existed between possession of marijuana off-duty and the duties of a tax representative trainee. An exception to this general rule exists, however, for sworn peace officers and safety-sensitive positions, discussed more fully in the section on drug and alcohol testing.

Dible v. Chandler

In this case, a police officer sued his employer for terminating him because, while off duty, he operated a pornographic website that featured sexually explicit photographs and videos of his wife. The police officer took pains to keep the police out of the picture, "but because of other clues and information, it became publicly known that he was involved and that he was a police officer." The court held that despite the plaintiff's efforts to keep his affiliation with the police department a secret, there was a nexus between the police officer's activity and his employment, reasoning that "it can seriously be asked whether a police officer can ever disassociate himself from his powerful public position sufficiently to make his speech (and other activities) entirely unrelated to that position in the eyes of the public and his superiors." This language suggests that at least for some public employees, such as police officers, any off duty conduct will be deemed to have a "nexus" to his/her employment. [503]

San Diego Unified School District v. Commission on Professional Competence (Lampedusa) [504]

A California Court of Appeal found that a nexus existed between off-duty Internet postings of a middle school administrator and his performance as an educator.

Frank Lampedusa was a tenured dean of students in the San Diego Unified School District. He placed an ad on Craigslist stating that he wished to engage in sexual relations with another adult. The ad also contained pictures of Lampedusa's face and genitalia. However, the ad did not reveal Lampedusa's name nor his employment. An anonymous parent of a student reported the ad to the school police who notified the District's administration of Lampedusa's ad. The District placed Lampedusa on paid administrative leave and eventually terminated him for "evident unfitness for service" and "immoral conduct," under the Education Code.

Lampedusa appealed his termination to a three-member commission on professional competence. The commission ordered Lampedusa reinstated, reasoning that the District failed to establish a nexus between his conduct and his performance as an educator. The District appealed the decision to the trial court who also did not find a nexus between the off duty conduct and Lampedusa's work as an educator.

The Court of Appeal agreed with the school district's termination decision finding a sufficient nexus existed between the misconduct and the impact on Lampedusa's performance as an educator.

In reaching its decision, the Court of Appeal gave weight to the hearsay evidence of the anonymous parent complaint to find that the conduct had an adverse effect on students. Lampedusa's principal also testified that she lost confidence in Lampedusa's ability to serve as a role model for students, thus establishing an adverse effect on other educators. The Court also gave weight to the fact that the conduct was not remote in time and that Lampedusa served as an administrator and educator in a middle school at the time the ad was posted. Lampedusa's conduct was further aggravated by the fact that he posted graphic, pornographic photos, and obscene written material on a website open to the public, that he admitted to posting similar ads in the past, that he would probably post tamer ads in the future, and that he believed he had not done anything immoral.

The Court also relied on evidence that Lampedusa did not take responsibility for his conduct, but rather stated that he expected parents and students to take care not to look at such ads on Craigslist, which have both age restrictions and warnings that the content is explicit. Lampedusa also asserted that, if students saw his ad, it would not affect his ability to teach them effectively.

The court found that Lampedusa's conduct was immoral because it evidenced indecency and moral indifference. The court further noted that disciplining Lampedusa for publicly posting his ad did not infringe on his constitutional rights or the rights of other teachers. These factors established evident unfitness for service.

Lampedusa was disciplined not for seeking a consensual sexual relationship with another adult but because he used poor judgment in a manner that affected his ability to serve as an administrator in a middle school.

i. Exception – Discussions about Union Activity or about Terms and Conditions of Employment

While employers may discipline employees for conduct on the internet that has a nexus to employment (see *San Diego Unified School District v. Commission on Professional Competence (Lampedusa)* above), employers should be careful not to discipline employees for complaints about the employee's terms and conditions of employment. Several National Labor Relations Board (NLRB) complaints address whether employees may be disciplined for information that the employees post on their Facebook pages when the information relates to the terms and conditions of employment.[505] Section 7 of the National Relations Act gives both unionized and non-unionized employees the right to discuss the terms and conditions of their employment with co-workers and others. This includes conducting Section 7 activity through use of employer email systems during non-working hours.[506]

LCW Practice Advisor

In California, employers should also note that California Labor Code sections 232 and 232.5 prohibits employers from taking adverse actions against employees for disclosing the amount of their wages and working conditions. Accordingly, we recommend that employers consider the context of employee speech in social media.

In *Purple Communications, Inc. v. Communications Workers of America, AFL-CIO*, the NLRB determined that employees who have been given access to an employer's email system in the course of their work are entitled to use system to engage in Section 7 activities during non-working hours.[507] An employer can rebut this presumption by showing that special circumstances make the ban necessary to maintain production or discipline.[508] An employer may also institute controls to the extent the controls are necessary to maintain production or discipline and the controls are applied uniformly and consistently enforced.[509]

In a report from the Acting General Counsel of the NLRB dated August 18, 2011[510], the Acting General Counsel found the following were concerted protected activities: a Facebook discussion between 5 coworkers about their job performance and workload; employee negative remarks about a supervisor who refused her request for union representation during an investigatory interview (*NLRB v. Hispanics United of Buffalo (New York)*[511]*)*; employee criticism and concerns about food at a sales events because it could affect his commission (*NLRB v. Knauz BWM*[512]); and an employee postings about employer tax withholding practices.

On the other hand, the NLRB has noted that speech involving individual gripes or "unprofessional and inappropriate tweets" that did not involve concerted activity was not protected by the NLRA.[513] In two 2017 cases involving Butler Medical Transport LLC, the NLRB made a distinction between comments about conditions that are of mutual concern to employees and posts that are "maliciously untrue and made with the knowledge that they are false."[514] In the case of the later, the employer was able to show that at the time the employee posted his complaint about his work vehicle breaking down, the employee was in private vehicle

and not a Butler ambulance.[515] The ALJ concluded that an employee's public criticism of his/her employer loses its protection under the Act if the statements are maliciously untrue even if the statements might have otherwise had protection under the Act.[516]

The NLRB has recognized the absence of precedent in cases involving "employer rules prohibiting, or disciplining employees for engaging in, protected concerted activity using social media, such as Facebook or Twitter," and that this absence of clear guidelines may create inconsistent results.[517] Agencies should therefore proceed with caution before disciplining employees for on-line comments.

Both the NLRB's May 30, 2012 report and its March 18, 2015 report focus on whether certain social media policies violated the NLRA by being overbroad and thus impermissibly restricting protected activity.[518] In its March 18, 2015 report, the NLRB provided guidance on what types of policies and rules would be permitted and not permitted under Section 7. For example:

- While an employer may not restrict employees from discussing employee information outside of work, it may ban the disclosure of its own confidential information as long as the restriction is narrowly limited.
- An employer cannot require employees to be respectful to the company or to managers/ supervisors, it can require employees not to be insubordinate.
- An employer can require employees to be respectful to customers or competitors, and direct employees not to engage in unprofessional conduct, as long as it does not prohibit criticism against management or the company.
- While an employer may prohibit employees from speaking as official company representatives, it may not prohibit employees from speaking to outsiders on their own behalf.
- An employer may not prohibit employees from using their personal devices to take pictures or recordings at work during non-work time.
- An employer may not prohibit an employee from walking off the job although it may advise that entering or leaving employer property without permission may result in discharge.
- An employer may have narrowly tailored conflict of interest rules if their context and examples demonstrate that they are not meant to apply to protected activity (e.g., designed to protect against employee graft, etc.).[519]

In addition, a 2013 NLRB cases held that an employer may not prohibit an employee from using Facebook during work time.[520] The reasoning is that the employee has breaks and is allowed to engage in protected activity during those breaks. An employer may also not prohibit an employee from airing work-related complaints on Facebook or prohibit employees from disclosing salary information or making inflammatory comments.[521] An employee may also use work email to send a message about a desired change in work conditions as part of protected activity.[522]

A 2014NLRB case has also held that an employer may not have a broadly defined confidentiality and non-disclosure policy that prohibits disparaging statements about the employer or that harm the reputation of the employer, and does not specify the types of disclosures that would be permissible.[523]

The NLRB does not have jurisdiction over public employers in California. The Public Employment Relations Board (PERB) is charged with administering the collective bargaining statutes governing California public employees, and would likely look to the NLRB for guidance on social media issues. Employers should seek legal counsel before disciplining employees when their social media communications involve protected activity, including discussions about union activity or the terms and conditions of employment, even when the posts also involve derogatory comments that may violate the employer's policies.

ii. Exception – Freedom of Expression Speech Protected by California Constitution and First Amendment

Freedom of expression is protected by the First Amendment of the United States Constitution, as made applicable to the states by the Fourteenth Amendment. (*Stanley v. Georgia* (1969) 394 U.S. 557, 559.) "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ." (U.S. Const., Amend. I.)

The California Constitution also protects the right of free speech. It provides:

"Every person may freely speak, write and publish his or her sentiments on all subjects, being responsible for the abuse of this right. A law may not restrain or abridge liberty of speech or press." (Cal. Const., art. I, § 2, subd. (a).)

In the 1968 decision *Pickering v. Board of Education,* the United States Supreme Court made it clear that public employers generally cannot stifle the First Amendment rights their employees would otherwise enjoy as citizens in commenting on matters of public interest.[524] However, the Court also recognized that public employers have an interest in the effective and efficient fulfillment of their responsibilities.[525] Therefore, a public employer's ability to maintain workplace efficiency must be balanced against a public employee's interest as a citizen in commenting upon matters of public concern. The test in *Pickering* (which in 2014 the Ninth Circuit determined is applicable to speech by professors and teachers)[526] is: (1) whether the academic speech addresses matters of public concern and, if so, (2) whether the employee's interest in the speech outweighs the educational institution's interest in providing efficient public services.[527]

Starting with *Pickering v. Board of Education*[528] and evolving with *Connick v. Myers*[529] and *Garcetti v. Ceballos*[530], the United .States. Supreme Court has developed a balancing test to determine when a public employee can assert a First Amendment retaliation claim. Such claim can be asserted only if: (1) the public employee spoke on a matter of public concern, (2) the public employee spoke as a private citizen rather than as a public employee, i.e., if the speech was not a result of the employee's "official duties," and (3) if on balance, the government had no adequate justification for treating the employee as it did, i.e., the public employee's interest as a citizen in commenting upon matters of public concern outweighs the interest of the public employer in promoting the efficiency of its public services.[531] *Garcetti*, however, does not apply to academic speech, which follows the test in *Pickering*.[532]

In *Dahlia v. Rodriguez*, the Ninth Circuit held that a Burbank police detective could assert a First Amendment retaliation claim based on his complaints to superiors about alleged abusive interrogation tactics at his department.[533]

In *Ellins v. City of Sierra Madre*[534], the Ninth Circuit Court of Appeals determined that a police officer who serves as union president could state a First Amendment retaliation claim based on his union-related speech. The speech at issue included the officer successfully leading a vote of "no confidence" against his Police Chief, and the union's press releases about the vote criticizing the Chief's management style. The Ninth Circuit, while not deciding the facts, determined that there was enough evidence for the plaintiff's case to go to a jury. The Court found that there was enough evidence, if believed by the jury, to support that the speech at issue was not an "individual personal grievance" but essentially "collective" grievances raised by the union. The Court also held that the speech was outside of the officer's "official duties" because he was speaking as the union's President and not pursuant to "official duties."

In *Johnson v. Poway Unified School District*[535] the Ninth Circuit Court of Appeal held that a high school math teacher did not have a First Amendment right to place religious posters or otherwise "use his public position as a pulpit from which to preach his own views on the role of God" to the captive students in his mathematics classroom. The Poway Unified School District allowed teachers to place posters and other materials on the walls of their classrooms conveying messages completely of the individual teacher's choosing. Bradley Johnson, a math teacher, maintained in his classroom two banners, each approximately seven feet wide and two feet tall. One, striped in red, white and blue, contained the phrases: "In God We Trust," "One Nation Under God," "God Bless America," and "God Shed His Grace On Thee." A second banner quoted from the Declaration of Independence by stating "All Men Are Created Equal, They Are Endowed By Their Creator," and placed the word "Creator" in all uppercase letters. Johnson had taught at the school for 30 years. The first banner had been in his classroom for 25 years, and the second for 17 years.

In 2007, the District, concerned about a violation of principles of separation of church and state ordered that Johnson remove the banners. Johnson sued alleging his First Amendment free speech rights had been violated. The Court of Appeal reversed the trial court holding that Johnson had no free speech claim. The Court held that for public high school teachers in this

context, "forum analysis" must give way to the specific framework the U.S. Supreme Court has developed for public employee speech claims. That framework asks, among other things, whether the employee spoke as a private citizen rather than a public employee. An employee speaks as a public employee when the speech is made pursuant to "official duties." In those circumstances, there is no First Amendment free speech claim.

The Court held that Johnson's banners constituted his speech as a public employee. The Court applied the following standard for making this determination for a teacher, in this particular case: "[B]ecause of the position of trust and authority they hold and the impressionable young minds with which they interact, teachers necessarily act as teachers for purposes of [an "official duties" analysis] when [they are] at school or a school function, in the general presence of students, in a capacity one might reasonably view as official."

The Court determined that Johnson's banners were pursuant to his "official duties" under this standard: "An ordinary citizen could not have walked into Johnson's classroom and decorated the walls as he or she saw fit, anymore than an ordinary citizen could demand that students remain in their seats and listen to whatever idiosyncratic perspective or sectarian viewpoints he or she wished to share."

The United States Supreme Court in *Borough of Duryea v. Guarnieri*[536], held that public employees cannot assert retaliation claims based upon the First Amendment right to petition unless their 'petitioning" in question involves a matter of public concern. A "petition" can be a grievance or lawsuit; however, a constitutional retaliation claim will arise only if the petition involves something sufficiently important to the general public.

As indicated above, free expression analysis is complex and fact-intensive. For a more in-depth discussion on freedom of expression please refer to Liebert Cassidy Whitmore's *Free Expression* workbook.

iii. Exception – Fair Labor Standards Act Anti-Retaliation Provision

The federal Fair Labor Standards Act ("FLSA") regulations the payment of wages including overtime wages to public employees. It contains an anti-retaliation provision, which provides that it is unlawful for an employer:

> *To discharge or in any manner discriminate against any employee because such employee has filed any complaint or instituted or caused to be instituted any proceeding under or related to [the FLSA], or has testified or is about to testify in such proceeding, or has served or is about to serve on an industry committee.*[537]

According to the U.S. Supreme Court, this anti-retaliation provision extends to both written and verbal complaints.[538] However, the complaint must be "sufficient clear and detailed for a reasonable employer to understand it, in light of both con ent and context, as an assertion of

rights protected by the statute and a call for their protection."[539] While this requirement may be met by an "informal workplace grievance procedure," a federal district court in Florida in 2011 refused to extend the FLSA anti-retaliation provision to a Facebook posting.[540] The court ruled that the Facebook posting was not a serious complaint but a "letting off steam" by the employee "simply voic[ing] her disagreement with her employer's payment practices on her Facebook page."[541] The court ruled this was not sufficient for a complaint, as an employer must have "'fair notice that an employee 'is in fact making a complaint about an Act violation, rather than just letting off steam.'[542]

b. Investigations into Off-Duty Conduct

Unreasonable and highly intrusive investigations into off-duty conduct can violate employees' rights to privacy.[543] Courts look to various factors to determine whether an investigation is unreasonable. The factors include the following:

- whether the means used in the investigation are abnormal; and
- whether the employer's purpose in conducting the investigation is proper.

It is not a violation of privacy to follow someone or watch him/her in public because there is no reasonable expectation of privacy while one is in public domain. This includes viewing information posted on website(s) such as Facebook, LinkedIn or Twitter when the postings are unrestricted and accessible or open to the general public.[544] Further, there is no violation of privacy involved when others willingly volunteer information.[545]

In a 2013 federal court decision outside of California[546], the court held that while the Stored Communications Act ("SCA") applied to Facebook postings meant to be kept private, it does not apply if the disclosure is by the intended user or recipient of the posting. One of an employee's Facebook friends voluntarily took screen shots of a Facebook posting and gave them to management. Management had not requested copies of the postings or asked the friend to spy on the employee. The employee was disciplined as a result of the postings. The court held that management's obtainment of the posting (initiated by and voluntarily undertaken by the employee's friend) did not violate the SCA.

> ***Note:*** *In California, Labor Code section 980 prohibits an employer from requiring or requesting that an applicant or employee disclosure his/her user name or password to the employer for the purpose of accessing the individuals' personal social media.[547] An exception exists when the employer reasonably believes the social media is relevant to an investigation of employee misconduct or employee violation of applicable laws and regulations and the social media is used solely for the purpose of the investigation or related proceeding.[548]*

Separate and apart from privacy concerns, however, caution should be exercised in determining the accuracy and reliability of information available from such public sources as the internet. Not everything posted in a blog or social networking site about a person is true; also not everything which appears to be attributable to a person is necessarily from the person. The spread of false information about individuals in the internet is rampant and could serve to undermine the reasonableness of an employer's reliance on that information as an accurate reflection of the employee's off-duty conduct.

An employer may legitimately investigate an employee's off-duty conduct which is believed to be in violation of legal statutes or the employer's rules or regulations. It would also be reasonable for an employer to investigate an employee's off-duty conduct to determine matters which have been placed at issue between the employer and employee in a legal proceeding. This could include such things as level and extent of disability, or need for or use of medical leave.

c. Lost Wages Claims Arising from Discipline for Off-Duty Conduct

Employees may file a claim with the Labor Commissioner under Labor Code section 96 for lost wages "as the result of demotion, suspension or discharge from employment for lawful conduct occurring during non-working hours away from the employer's premises."[549]

All public employers should assume that Labor Code section 96, subdivision (k), applies to them until or unless a court rules definitively otherwise. Section 96 does not set forth an independent public policy that provides employees with substantive rights.[550] The statute simply outlines types of claims over which the Labor Commissioner shall exercise jurisdiction; therefore the statute does not support a claim of wrongful termination in violation of public policy.[551] In 2000, the California Attorney General issued an opinion that Section 96 does not abrogate existing law that permits law enforcement agencies to discipline peace officers for lawful off-duty conduct occurring away from the workplace which conflicts with their duties as peace officers.[552]

A myriad of federal and state statutes protect civil rights. Accordingly, the job-nexus analysis outlined above still applies when deciding whether to discipline an employee for off-duty conduct.

2. OUTSIDE EMPLOYMENT

Employees generally do not have the right to engage in outside employment which adversely impacts upon the employees' regular position. Government Code section 1126 sets forth the necessary nexus for limiting employees' outside employment. Section 1126 provides as follows:

> *"[A] local agency officer or employee shall not engage in any employment, activity, or enterprise for compensation which is inconsistent, incompatible, in conflict with, or inimical to his or her duties…or with the duties, functions, or responsibilities of his or her appointing power or the agency."*

"Each appointing power may determine…those outside activities which…are inconsistent with, incompatible to, or in conflict with their duties as local agency officers or employees."

Incompatibility may be found in the following circumstances, but is not limited to these circumstances:

- employee uses local agency time, facilities, property, or influence for private gain;
- employee accepts or receives compensation for performing the duties required by his or her position other than from the local agency;
- employee performs an act which may later be subject to direct or indirect control, inspection, review, audit, or enforcement of another officer or employee of the local agency; or
- the outside employment involves time demands that would render performance of the duties of the normal position less efficient.[553]

A local agency may adopt rules specifying prohibited activities. In *Long Beach Police Officer Ass'n v. City of Long Beach*,[554] the California Supreme Court upheld a local agency rule which prohibited police officers from engaging in outside employment which involved serving civil process or assisting in civil cases.

The court held that under section 1126, the specification of activities which "may be prohibited" was intended to guide rather than confine the local agency's exercise of its authority. Thus, a city is entitled to proscribe incompatible employment even though it is not specifically delineated in the statute.

Local agencies should be aware of Penal Code section 70 which specifically authorizes peace officers to be employed as security guards or patrol officers while off duty. It also permits peace officers to perform peace officer functions concurrent with the off-duty position, provided they wear their police uniform, the employer has approved the off-duty position, and the peace officer follows the agency employer's rules and regulations. Although agencies may still deny off-duty security guard work on the basis of Government Code section 1126 or for other business-related reasons, amendments to section 70 require the local agency to provide those reasons in writing to the peace officer. Employers should note the requirement to provide those reasons in writing to the peace officer. Employers should note that the requirement to provide written reasons for denial applies to any off-duty work, not just security guard work.
555

3. SMOKING

Generally, smoking in the workplace encompasses two different issues:

- What obligation does an employer have to accommodate the rights of non-smokers; and
- Can employers ban employees from smoking altogether, both on- and off-duty.

a. The Rights of Non-Smokers

Many states and municipalities have adopted smoking restrictions in the workplace that apply to both public and private employers. These statutes and ordinances impose a duty on employers to minimize a worker's exposure to smoke.

In enacting Labor Code section 6404.5, the California Legislature intended to prohibit the smoking of tobacco products in all enclosed places of employment. Only certain facilities are excluded from this restriction.[556] But places which are not covered by section 6404.5 are subject to local regulation.[557]

Under Government Code section 19994.30 *et seq*, smoking is not allowed inside or in an outdoor area within five feet of a main entrance or exit to any state-owned, occupied or state-leased and occupied building or in passenger vehicles owned by the state.

With regard to public buildings, the California Attorney General has opined that counties have the right to enact ordinances banning all smoking in county buildings, and may enforce them against members of the public within their incorporated territories.[558]

Beyond state laws and local ordinances, federal court decisions have held that an employee who is unusually sensitive to tobacco smoke is "handicapped" within the contemplation of section 504 of the Rehabilitation Act of 1973, Title 29 United States Code section 794. Courts have held that someone with such a condition is physically handicapped within the protection of the FEHA.[559] As a result, employers are now under a duty to reasonably accommodate the needs of those who are sensitive to cigarette smoke.[560]

b. Employer's Right to Prohibit Employees from Smoking Altogether

Whether employers can prohibit employees from smoking both on and off-duty is generally related to the issue of an employer's right to regulate off-duty conduct. In most situations, it is unlikely that employers may prohibit smoking away from the work site. However, certain professions, such police officers, are justifiably expected to maintain high standards of physical fitness due to the unique rigors of this kind of work.

According to a decision by the California Public Employment Relations Board, a school district was not required to negotiate prior to implementing a policy that banned smoking in all District buildings and vehicles, and at District-sponsored activities, whether such activities occurred on or off District premises. The District had been motivated by several factors, including Education Code section 48901 which requires discouragement of high school students from smoking.[561]

The Americans with Disabilities Act, and the California Fair Employment and Housing Act may prohibit an employer from refusing to hire smokers who are qualified to perform the essential functions of the job for which they apply. Although smoking, unlike rehabilitated illegal drug addiction, is not a protected disability enumerated in the ADA, it may nevertheless be covered if the employer regards it as a substantially limiting impairment or if the employer's attitude renders it a substantially limiting impairment.[562] A non-smoking regulation could be subject to a credible legal challenge under the Americans with Disabilities Act, Fair Employment and Housing Act, and under California's constitutional right to privacy.

4. GROOMING STANDARDS

An employer can establish reasonable dress codes for its employees. To avoid violating the discrimination laws, however, the dress codes should be uniformly applied to men and women. This does not mean that they need to be identical; they must, however, impose an equal standard or burden.[563]

According to the DFEH in guidance provided on Transgender Right in the Workplace, "unless an employer can demonstrate business necessity, each employee must be allowed to dress in accordance with their gender identity and gender expression."[564] "Transgender or gender non-conforming employees may not be held to any different standard of dress or grooming than any other employee."[565]

A police department has been held to be able to establish hair grooming standards for male members of the police force. In *Kelley v. Johnson*,[566] the court held that a county's hair grooming regulation for its police officers was not so irrational that it could be branded arbitrary and thus a deprivation of a police officer's liberty interest in the freedom to choose his own hairstyle.

Thus, an employer may enact certain grooming standards if they have a rational connection to the organizational needs of the workforce, as well as the protection of persons and property. Nonetheless, caution is advised in enacting such policies on this basis. In one case, the court determined that a fire department's ban on facial hair discriminated against persons with "folliculitis barbae," or razor-bumps, a handicap. The department's safety rationale, that facial hair could cause a mask to leak, was insufficient evidence of a safety risk. According to the court, a reasonable accommodation would allow wearing of a beard and required frequent tests of a firefighter's safety mask.[567]

Education Code section 35183 provides that a school district governing board may adopt reasonable dress code regulations prohibiting students from wearing gang-related apparel if deemed necessary for health and safety purposes.

5. RESIDENCY RESTRICTIONS

An employer has limited authority to regulate/restrict where its employees reside pursuant to Article XI, Section 10, Subdivision (b) of the California Constitution which provides that while a local agency may not require that employees be residents of the city or county, it may require employees to reside within a reasonable distance of their place of employment.

> ***International Ass'n of Fire Fighters Local 55 v. City of San Leandro,***[568]
> An appellate court held that a city requirement that fire department personnel reside within 40 miles from a fire station was not so unreasonable as to be constitutionally defective, even though it did not provide for consideration of the firefighters' individual travel time from their residences.

6. LANGUAGE

Under FEHA, Government Code Section 12951, employers are barred from adopting or enforcing a policy that prohibits the use of any language in the workplace unless: (i) the policy is justified by business necessity; and (ii) the employer provides the employees with adequate notice of the policy and the consequences of violating the policy.

Policies prohibiting the use of any language are reviewed under a stringent standard. Section 12951(b) requires that the employer show (i) "an overriding legitimate business purpose" that makes the language restriction "necessary to the safe and efficient operation of the business," (ii) that the restriction fulfills the business purpose, and (iii) that there is "no alternative practice to the language restriction that would accomplish the business purpose equally well with a lesser discriminatory impact." Importantly, employers are subject to Section 12951 even if the policy is verbal, and not reduced to writing. Employers cannot verbally threaten employees with discipline, or any other adverse action, for speaking in languages other than English. Any policy, whether verbal or written, will subject the employer to liability under Section 12951.

Section 12951 became effective in 2002. Thus, employers should not rely on case law decided before Section 12951 was enacted in developing language restriction policies. Cases that were decided prior to its enactment would likely have a different outcome in light of Section 12951.

7. MEDIA ATTENTION

Under Government Code section 3303(e), the employer [law enforcement agency] must not cause the public safety officer under interrogation to be subjected to visits by the press or news media without his expressed consent nor shall his home address or photograph be given to the press or news media without his expressed consent.

8. FINANCIAL STATUS

Given the right of privacy, employers must have a job-related reason for inquiring into an employee's financial status.

Under Government Code section 3308, no peace officer can be required or requested for purposes of job assignment or other personnel action to disclose any item of his or her property, income, assets, source of income, debts or personal or domestic expenditures (including those of any member of his or her family or household) unless:

- Such information is obtained or required under state law or proper legal procedures;
- Tends to indicate a conflict of interest with respect to the performance of his or her official duties; or
- Is necessary for the employing agency to ascertain the desirability of assigning the public safety officer to a specialized unit in which there is a strong possibility that bribes or other improper inducements may be offered.

These conditions are not conjunctive; therefore, any one of them allows the employer to require the disclosure.

C. USE OF IMAGE OR LIKENESS

The common law tort of misappropriation of image and/or likeness prohibits an entity or employer from using someone's name or likeness for commercial purposes without his or her consent. Thus, if an agency publishes the likenesses of a student or employee on the agency's website without consent, the agency risks receiving a claim for misappropriation of image and/or likeness under the common law.

In addition, under California law, the agency may be liable for misappropriation of image and/or likeness under a statutory provision, Civil Code section 3344. Civil Code section 3344 protects an individual's name, voice, signature, photograph, or likeness, from being used for commercial or advertising purposes without consent. Civil Code section 3344 also authorizes the recovery of damages for violation of its provisions. Potential damages for a violation of Civil Code section 3344 are the greater of seven hundred fifty dollars ($750) or the actual damages suffered; punitive damages; and attorney's fees and costs.

To avoid potential exposure under the common law and/or Civil Code section 3334, we recommend that agencies do not use the photographs, images, or likeness of employees on the agencies' web site, billboards or other publicity tool without first obtaining consent to do so.

ENDNOTES

[1] *National Aeronautics and Space Administration v. Nelson* (2011) 562 U.S. 134 [131 S.Ct. 746] *Whalen v. Roe* (1977) 429 U.S. 589 [97 S.Ct. 869].

[2] *Griswold v. Connecticut* (1965) 381 U.S. 479 [85 S.Ct. 1678]; *Whalen v. Roe* (1977) 429 U.S. 589, 599 [97 S.Ct. 869].

[3] *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459; *see also Eisenstadt v. Baird* (1972) 405 U.S. 438 [92 S.Ct. 1029]; *Roe v. Wade* (1973) 410 U.S. 113 [93 S.Ct. 705] (basic matters as contraception, abortion, marriage, and family life are protected by the constitution from unwarranted government intrusion).

[4] *Waters v. Churchill* (1994) 511 U.S. 661 [114 S.Ct. 1878]; *Heffernan v. City of Paterson, N.J.* (2016) 136 S. Ct. 1412.

[5] Cal. Const., art. I, § 1.

[6] *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1 [26 Cal.Rptr.2d 834].

[7] *Williams v. Superior Court* (2017) 3 Cal.5th 531.

[8] *Williams v. Superior Court* (2017) 3 Cal.5th 531, 556.

[9] *Kapellas v. Kofman* (1969) 1 Cal.3d 20 [81 Cal.Rptr. 360].

[10] Gov. Code, §§ 810, 815.

[11] *Miklosy v. Regents of the University of California* (2008) 44 Cal.4th 876, 899 [80 Cal.Rptr.3d 690].

[12] *Forsher v. Bugliosi* (1980) 26 Cal.3d 792 [163 Cal.Rptr. 628]; *Sipple v. Chronicle Publishing Co*. (1984) 154 Cal.App.3d 1040 [201 Cal.Rptr. 665].

[13] *Porten v. University of San Francisco* (1976) 64 Cal.App.3d 825 [134 Cal.Rptr. 839].

[14] *Ignat v. Yum! Brands, Inc.* (2013) 214 Cal.App.4th 808 [154 Cal.Rptr.3d 275].

[15] *Tecza v. University of San Francisco*, 2013 WL 3186572 (unpublished).

[16] *Institute of Athletic Motivation v. University of Illinois* (1980) 114 Cal.App.3d 1 [170 Cal.Rptr. 411]; Civ. Code § 47, subd. (c).

[17] Civ. Code, § 47, subd. (c); *Taus v. Loftus* (2007) 40 Cal.4th 683, 721

[18] *Deaile v. General Telephone Co. of California* (1974) 40 Cal.App.3d 841 [115 Cal.Rptr. 582].

[19] *Comeaux v. Brown & Williamson Tobacco Co.* (1990) 915 F.2d 1264; *Emerson v. J.F. Shea Co.* (1978) 76 Cal.App.3d 579 [143 Cal.Rptr. 170].

[20] *Lorenzana v. Superior Court* (1973) 9 Cal.3d 626 [108 Cal.Rptr. 585]; *Gill v. Hearst Pub. Co.* (1953) 40 Cal.2d 224 [253 P.2d 441].

[21] *Pettus v. Cole* (1996) 49 Cal.App.4th 402, 442–43 [57 Cal.Rptr.2d 46, 73–74], as mod. on den. of rehg., review den.

[22] *Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia* (3rd Cir. 1987) 812 F.2d 105, decision vacated (3rd Cir. 1988) 859 F.2d 276.

[23] Indeed, in a case discussing *Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia* (3rd Cir. 1987) 812 F.2d 105, a California Court of Appeal recognized that peace officers who seek to be promoted or transferred to specialized divisions whose work is unusually sensitive or requires high integrity can be subject to polygraph examinations. *Los Angeles Police Protective League v. City of Los Angeles* (1995) 35 Cal.App.4th 1535 [42 Cal.Rptr.2d 23]. Presumably, the employer also has greater latitude in applicant questioning for such positions

because of the sensitivity of work at issue and the greater likelihood of job nexus for different types of questions.

[24] *National Aeronautics and Space Administration v. Nelson* (2011) 562 U.S. 134 [131 S.Ct. 746].

[25] *National Aeronautics and Space Administration v. Nelson* (2011) 562 U.S. 134 [131 S.Ct. 746, 761].

[26] 5 U.S.C. § 552(a). (Proposed Legislation)

[27] *National Aeronautics and Space Administration v. Nelson* (2011) 562 U.S. 134 [131 S.Ct. 746, 762].

[28] *National Aeronautics and Space Administration v. Nelson* (2011) 562 U.S. 134 [131 S.Ct. 746, 762].

[29] *National Aeronautics and Space Administration v. Nelson* (2011) 562 U.S. 134 [131 S.Ct. 746, 762].

[30] DFEH, Transgender Rights in the Workplace (November 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/11/DFEH_E04P-ENG-2017Nov.pdf.

[31] DFEH, Transgender Rights in the Workplace (November 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/11/DFEH_E04P-ENG-2017Nov.pdf.

[32] DFEH, Transgender Rights in the Workplace (November 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/11/DFEH_E04P-ENG-2017Nov.pdf.

[33] See Moreno v. Hanford Sentinel, Inc. (2009) 172 Cal.App.4th 1125 [91 Cal.Rptr.3d 858], as mod., where California Court of Appeal held that an article posted on MySpace.com was not private and could not be republished without the author's permission.

[34] Lab. Code, § 980.

[35] Lab. Code, § 1198.5.

[36] *Board of Trustees v. Superior Court* (1981) 119 Cal.App.3d 516 [174 Cal.Rptr. 160]; disapproved of on other grounds by *Williams v. Superior Ct.* (2017) 3 Cal.5th 531..

[37] 15 U.S.C. § 1681g(2). (Proposed Legislation)

[38] Civ. Code, § 1786.10, subd. (b).

[39] *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459, cert denied (1984) 469 U.S. 979 [105 S. Ct. 380, 383] and appeal after remand (1986) 802 F.2d 1131, disagreed with (E.D. Mich. 2000) 81 F.Supp.2d 814.

[40] *Johnson v. Winter* (1982) 127 Cal.App.3d 435 [179 Cal.Rptr. 585].

[41] Gov. Code, §§ 6250 et seq.

[42] *Johnson v. Winter* (1982) 127 Cal.App.3d 435, 438-439 [179 Cal.Rptr. 585, 588] *(emphasis supplied)*.

[43] *Comeaux v. Brown & Williamson Tobacco Co.* (9th Cir 1990) 915 F.2d 1264.

[44] *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459, cert. den. (1984) 469 U.S. 979 [105 S.Ct. 380] and appeal after remand (9th Cir. 1986) 802 F.2d 1131, disagreed with (E.D. Mich. 2000) 81 F.Supp.2d 814.

[45] 15 U.S.C. § 1681-1681u. (Proposed Legislation)

[46] Civ. Code, §§ 1785.1-1785.6.

[47] *Griggs v. Duke Power Co*. (1971) 401 U.S. 424, 432 [91 S.Ct. 849, 853-854], implied overruling of Griggs' disparate impact analysis in a statutory context requiring intentional discrimination recognized by (9th Cir. 1996) 914 F.Supp. 1257.

[48] 15 U.S.C. §§ 1681 et seq. (Proposed Legislation)

[49] 15 U.S.C. §§ 1681a(d)(1)(A)-(C). (Proposed Legislation)

[50] 15 U.S.C. § 1681a(f). (Proposed Legislation)

[51] 15 U.S.C. § 1681a(f). (Proposed Legislation)

[52] 15 U.S.C. §§ 1681n, 1681o. (Proposed Legislation)

[53] *See, e.g.*, 15 U.S.C. § 1681m(c). (Proposed Legislation)

[54] 15 U.S.C. § 1681b(b)(2)(A). (Proposed Legislation)

[55] 15 U.S.C. § 1681b(b)(2)(B). (Proposed Legislation)

[56] 15 U.S.C. § 1681b(b)(1)(A). (Proposed Legislation)
[57] 15 U.S.C. § 1681b(g). (Proposed Legislation)
[58] 15 U.S.C. § 1681a(k)(1)(B)(ii). (Proposed Legislation)
[59] 15 U.S.C. § 1681b(c). (Proposed Legislation)
[60] 15 U.S.C. § 1681m(a). (Proposed Legislation)
[61] 15 U.S.C. § 1681b(f)(1). (Proposed Legislation)
[62] 15 U.S.C. § 1681c. (Proposed Legislation)
[63] 15 U.S.C. § 1681c(b). (Proposed Legislation)
[64] 15 U.S.C. § 1681b(g). (Proposed Legislation)
[65] Civ. Code, § 1786 et seq.
[66] Civ. Code, § 1786.53.
[67] Civ. Code, § 1786.20, subd. (d).
[68] Civ. Code, § 1786.2, subd. (c).
[69] Lab. Code, § 1024.5 (effective January 1, 2012).
[70] Civ. Code, § 1786.10, subd. (b)(1).
[71] Civ. Code, § 1786.16, subd. (a)(2)(B).
[72] Civ. Code, § 1786.16, subd. (b)(1).
[73] Civ. Code, § 1786.16, subd. (a)(2)(C); Civ. Code, § 1786.12, subds. (c), (f).
[74] Civ. Code, § 1786.18, subd. (a)(4).
[75] Civ. Code, § 1786.40.
[76] Civ. Code, § 1786.24.
[77] Civ. Code, § 1786.24.
[78] Civ. Code, § 1786.18, subd. (a).
[79] Civ. Code, § 1786.18, subd. (d).
[80] Civ. Code, § 1786.53, subd. (b)(2).
[81] Civ. Code, § 1786.53, subd. (b)(1).
[82] Civ. Code, § 1786.53, subd. (b)(4).
[83] Civ. Code, § 1786.53, subd. (b)(2).
[84] Gov. Code, § 12952(a)(1)-(4).
[85] Gov. Code, § 12952(b).
[86] Gov. Code, § 12952(d)(1)-(4).
[87] Gov. Code, § 12952(c)(1)(A).
[88] Gov. Code, § 12952(c)(1)(A)(i)-(iii).
[89] Gov. Code, § 12952(c)(1)(B).
[90] Gov. Code, § 12952(c)(2).
[91] Gov. Code, § 12952(c)(2).
[92] Gov. Code, § 12952(c)(2)(A)-(C).
[93] Gov. Code, § 12952(c)(3).
[94] Gov. Code, § 12952(c)(4).
[95] Gov. Code, § 12952(c)(5)(A)-(C).
[96] Gov. Code, § 12952(d)(4).
[97] Lab. Code, §§ 432.7, 432.8.

[98] *Starbucks Corp. v. Superior Court* (2008) 168 Cal.App.4th 14361436 [86 Cal.Rptr.3d 482], review den.

[99] Lab. Code, §§ 432.7, subds. (a), (d) & (e), 432.8.

[100] Lab. Code, § 432.9, subd. (a).

[101] Lab. Code, § 432.9, subd. (a).

[102] Lab. Code, § 432.9, subd. (c).

[103] Lab. Code, § 432.9, subd. (b).

[104] Lab. Code, § 432.9, subd. (b).

[105] U.S. Equal Opportunity Commission, EEOC Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions under Title VII of the Civil Rights Act of 1964, Number 915.002 (April 25, 2012).

[106] U.S. Equal Employment Opportunity Commission, Questions and Answers about the EEOC's Enforcement Guidance on the Consideration of Arrest and Convictions Records in Employment Decisions under Title VII April, 2012, Question 1.

[107] U.S. Equal Employment Opportunity Commission, Questions and Answers about the EEOC's Enforcement Guidance on the Consideration of Arrest and Convictions Records in Employment Decisions under Title VII, April 2012, Question 7.

[108] U.S. Equal Employment Opportunity Commission, Questions and Answers about the EEOC's Enforcement Guidance on the Consideration of Arrest and Convictions Records in Employment Decisions under Title VII, April 2012, Question 7.

[109] *Long Beach City Employees Assn. v. City of Long Beach* (1986) 41 Cal.3d 937 [227 Cal.Rptr. 90].

[110] *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459, cert. den. (1984) 469 U.S. 979 [105 S.Ct. 380, 383], and appeal after remand (9th Cir. 1986) 802 F.2d 1131, disagreed with (E.D. Mich. 2000) 81 F.Supp.2d 814.

[111] *Los Angeles Police Protective League v. City of Los Angeles* (1995) 35 Cal.App.4th 1535 [42 Cal.Rptr.2d 23].

[112] *Estes v. City of Grover City* (1978) 82 Cal.App.3d 509 [147 Cal.Rptr. 131].

[113] *Aengst v. Board of Medical Quality Assurance* (1980) 110 Cal.App.3d 275 [167 Cal.Rptr. 796].

[114] *Los Angeles Police Protective League v. City of Los Angeles* (1995) 35 Cal.App.4th 1535 [42 Cal.Rptr.2d 23].

[115] Civ. Code, § 44.

[116] 5 Witkin, Summary of Cal. Law (9th ed. 1988) Torts § 402, p. 618.

[117] 5 Witkin, Summary of Cal. Law (9th ed. 1988) Torts § 652, pp. 958-959.

[118] Lab. Code, §§ 1050, 1054.

[119] *Bardin v. Lockheed Aeronautical Systems Co.* (1999) 70 Cal. App.4th 494 [82 Cal.Rptr.2d 726], rehg. den.; *Conkle v. Jeong* (N.D. Cal. 1994) 853 F.Supp. 1160, cert. den. (1996) 519 U.S. 811 [117 S.Ct. 56].

[120] *McQuirk v. Donnelley* (9th Cir. 1999) 189 F.3d 793.

[121] 29 C.F.R. § 1602.49.

[122] Labor Code, § 1019.2(a).

[123] Labor Code, § 1019.2(b)(1) and (2).

[124] Labor Code, § 1019.2(c).

[125] Civ. Code, § 56.05, subd. (g).

[126] Gov. Code, §§ 12940 et seq.

[127] 29 U.S.C. §§ 651-678. (Proposed Legislation)

[128] See 29 C.F.R. §§ 1635.8(a), (b)(1)(ii)(A)-(D).

[129] Federal Register, Volume 78, Issue 17 (Friday, January 25, 2013); see also 45 C.F.R. §§160.103; (Proposed Regulation) 164.502(a)(5)(i).

[130] Breach Notification for Unsecured Protected Health Information, 74 Fed.Reg. 42740 (Aug. 24, 2009). More information regarding the U.S. Department of Health and Human Service's regulations and a full copy of the regulations can be found at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html> (as of Jul. 4, 2011).

[131] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees Under the American with Disabilities Act (ADA) (Jul. 2000).

[132] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations (Oct. 1995) p. 13

[133] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations (Oct. 1995) p. 13

[134] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability- Related Questions and Medical Examinations (Oct. 1995) p. 17

[135] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations (Oct. 1995) p. 17

[136] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations (Oct. 1995) p. 17-18

[137] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations (Oct. 1995) p. 18

[138] *Leonel v. American Airlines, Inc.* (9th Cir. 2005) 400 F.3d 702, opn. mod. on denial of rehg. (9th Cir.2005) 2005 WL 976985.

[139] 29 C.F.R. § 1630.14(a).

[140] 29 C.F.R. § 1630.3(b)(1); U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees under the American with Disabilities Act (ADA) (Jul. 2000) p.5.

[141] Cal. Code Regs., tit. 2, § 7294.0, subd. (b)(2).

[142] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability Related Questions and Medical Examinations (Oct. 1995) p. 16

[143] 42 U.S.C. § 12112(d)29 C.F.R. §1630.13(a); Cal. Code Regs., tit. 2, § 7294.0, subd. (b)(2).

[144] 42 U.S.C. § 12112(d) (Unconstitutional or Preempted, Proposed Legislation) 29 C.F.R. § 1630.13(a); Cal. Code Regs., tit. 2, § 7294.0, subd. (b)(2).

[145] Cal. Code Regs., tit. 2, § 7294.1, subd. (b)(2); *Lujan v. Pacific Maritime Assn.* (9th Cir. 1999) 165 F.3d 738, 742 [strength and agility tests for longshore worker not reasonably related to signal and clerk assignments].

[146] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees under the American with Disabilities Act (ADA) (Jul. 2000).

[147] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees under the American with Disabilities Act (ADA) (Jul. 2000).

[148] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees under the American with Disabilities Act (ADA) (Jul. 2000); Cal. Code Regs., tit. 2, § 7287.4, subd. (a).

[149] Gov. Code, § 12940, subd. (e)(3).

[150] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability Related Questions and Medical Examinations (Oct. 1995) pp.15-16

[151] Interpretative Guidance on Title 1 of the Americans with Disabilities Act, 29 C.F.R. § 1630 App. (2000).

[152] Interpretive Guidance on Title I of the Americans with Disabilities Act, 29 C.F.R. Pt. 1630, Appen. (2016).

[153] Interpretative Guidance on Title 1 of the Americans with Disabilities Act, 29 C.F.R. § 1630 App. (2000).

[154] Gov. Code, § 12940, subd. (e)(3).

[155] Cal. Code Regs., tit. 2, § 7294.0, subd. (d).

[156] U.S. Equal Empl. Opportunity Com., ADA Enforcement Guidance: Preemployment Disability Related Questions and Medical Examinations (Oct. 1995) p. 2,

[157] Gov. Code, § 12940, subd. (e)(3); Cal. Code Regs., tit. 2, § 7287.3, subd. (b)(1).

[158] Health & Saf. Code, § 120980, subd. (f).

[159] *Loder v. City of Glendale* (1997) 14 Cal.4th 846 [59 Cal.Rptr.2d 696], cert. den. 522 U.S. 807 [118 S.Ct. 44].

[160] Gov. Code, § 12940, subd. (f)(1).

[161] 42 U.S.C. § 12112(d)(4)(A)29 C.F.R. § 1630.14(c); Gov. Code, § 12940, subd. (f).

[162] Gov. Code, § 12940, subds. (e) & (n).

[163] Cal. Code Regs., tit. 2, § 7294.0, subd. (d).

[164] Cal. Code Regs., tit. 2, § 7293.8, subd. (c).

[165] *Equal Employment Opportunity Commission v. United Parcel Service, Inc.* (9th Cir. 2005) 424 F.3d 1060.

[166] *Norman-Bloodsaw v. Lawrence Berkeley Laboratory* (9th Cir. 1998) 135 F.3d 1260.

[167] Gov. Code, § 12940, subd. (f)(1).

[168] 42 U.S.C. § 12112(d)(4)(A) Gov. Code, § 12940, subd. (f)(2). **(Unconstitutional or Preempted, Proposed Legislation)**

[169] Gov. Code, § 12940, subd. (m).

[170] 42 U.S.C. § 12111(8), (9). **(Unconstitutional or Preempted, proposed Legislation)**

[171] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act (ADA) (Oct. 2002).

[172] Gov. Code, § 12940, subd. (f)(2).

[173] Civ. Code, § 56.10, subd. (c)(8)(B).

[174] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act (ADA) (Oct. 2002).

[175] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act (ADA) (Oct. 2002).

[176] U.S. Equal Empl. Opportunity Com., Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees under the American with Disabilities Act (ADA) (Jul. 2000) pp. 8-9.

[177] *Loder v. City of Glendale* (1997) 14 Cal.4th 846, 887-898 [59 Cal.Rptr.2d 696, 721-729], cert. den. 522 U.S. 807 [118 S.Ct. 44].

[178] 29 U.S.C. § 2613(a) (Proposed Legislation); Gov. Code, § 12945.2, subds. (j) & (k).

[179] 29 C.F.R. § 825.102(Unconstitutional or Preempted); 29 C.F.R. § 825.122(b).

[180] Cal. Code Regs., tit. 2, § 7297.0, subd. (a).

[181] Gov. Code, § 12945.2, subd. (c)(8); 29 U.S.C. § 2611(11).

[182] Gov. Code, § 12945.2, subd. (k)(1).

[183] 29 C.F.R. § 825.306(b)(1).

[184] Cal. Code Regs., tit. 2, § 7297.4, subd. (b)(2)(A)(1).

[185] Cal. Code Regs., tit. 2, § 7297.11.

[186] Gov. Code, § 12945.2, subd. (j)(1); Cal. Code Regs., tit. 2, § 7297.0, subd. (a)(1).

[187] Cal. Code Regs., tit. 2, § 7297.0, subd. (a)(1)(D)(1).

[188] 29 U.S.C. § 2613(b).(Proposed Legislation)

[189] Gov. Code, § 12945.2, subd. (k)(2).

[190] Gov. Code, § 12945.2, subd. (j)(2).

[191] 29 U.S.C. § 2613(e) (Proposed Legislation)29 C.F.R. § 825.308(a).

[192] 29 U.S.C. § 2613(c) (Proposed Legislation)Gov. Code, § 12945.2, subd. (k)(3)(A).

[193] 29 U.S.C. § 2613(c)(2) (Proposed Legislation); Gov. Code, § 12945.2, subd. (k)(3)(B).

[194] 29 U.S.C. § 2613(d)(1) (Proposed Legislation)Gov. Code, § 12945.2, subd. (k)(3)(C).

[195] 29 U.S.C. § 2613(d)(2) (Proposed Legislation)Gov. Code, § 12945.2, subd. (k)(3)(D).

[196] 29 U.S.C. § 2614(a)(4). (Proposed Legislation)

[197] Cal. Code Regs., tit. 2, § 7297.4, subd. (b)(2)(E).

[198] Cal. Code Regs., tit. 2, § 7291.10, subd. (b).

[199] Cal. Code Regs., tit. 2, § 7291.2, subd. (d).

[200] Cal. Code Regs., tit. 2, § 7291.10, subd. (b).

[201] Cal. Code Regs., tit. 2, § 7291.10, subd. (c).

[202] Lab. Code, § 3762, subd. (c)(1)-(2).

[203] 42 U.S.C. § 12112(d)(4)(A);29 C.F.R. § 1630.14(c); Gov. Code, § 12940, subd. (f).

[204] Interpretive Guidance on Title I of the Americans with Disabilities Act, 29 C.F.R. § 1630.

[205] *Yin v. State of California* (9th Cir. 1996) 95 F.3d 864, 873, cert. den. (1997) 519 U.S. 1114 [117 S.Ct. 955].

[206] *Yin v. State of California* (9th Cir. 1996) 95 F.3d 864, 868, cert. den. (1997) 519 U.S. 1114 [117 S.Ct. 955].

[207] *Sullivan v. River Valley School District* (6th Cir. 1999) 197 F.3d 804, 811, cert. den. (2000) 530 U.S. 1262 [120 S.Ct. 2718].

[208] 29 C.F.R. § 1910.1001(d), (e) (asbestos).

[209] 29 C.F.R. § 1910.134(e).

[210] 49 C.F.R. § 40.25.

[211] *Yin v. State of California* (9th Cir. 1996) 95 F.3d 864, cert. den. (1997) 519 U.S. 1114 [117 S.Ct. 955].

[212] *Deckert v. City of Ulysse*s, *Kan.* (10th Cir. 1996) 105 F. 3d 669.

[213] *Fritsch v. City of Chula Vista* (S.D.Cal. 2000) 2000 WL 1740914.

[214] *Jermon v. County of Sonoma* (N.D.Cal. 1997) 1997 WL 203703.

[215] Civ. Code, § 56.10, subd. (c)(8)(B).

[216] Civ. Code, § 56.10, subd. (c)(8)(B).

[217] Civ. Code, § 56.20, subd. (b).

[218] Civ. Code, § 56.20.

[219] Civ. Code, § 56.05, subd. (b).

[220] Civ. Code, § 56.20.

[221] 42 U.S.C. §§ 12101 et seq.

[222] 42 U.S.C. § 12112, subd. (d)(3)(B). (Unconstitutional or Preempted, Proposed Legislation)

[223] Civ. Code, § 56.05, subd. (g).

[224] Civ. Code, § 56.05, subd. (g).

[225] Civ. Code, § 56.11.

[226] Civ. Code, § 56.10, subds. (b) & (c).

[227] Civ. Code, § 56.20, subd. (d).

[228] 45 C.F.R. § 160.103. (Proposed Legisaltion)

[229] 45 C.F.R. § 164.103.

[230] 45 C.F.R. § 164.530.

[231] Civ. Code, § 56.20, subd. (c).

[232] Cal. Code Regs., tit. 8, § 3204, subd. (e)(1)(A).

[233] Code Civ. Proc., § 1985.3.

[234] Code Civ. Proc., § 1985.3, subd. (b).

[235] Fed. Rules Civ. Proc., rule 45(c)(2)(B); 28 U.S.C.

[236] Fed. Rules Civ. Proc., rule 45(c)(3); 28 U.S.C.

[237] Gov. Code, §§ 6250 et seq.

[238] Gov. Code, § 6254, subd. (c).

[239] Gov. Code, § 6253, subd. (c).

[240] Pen. Code, § 832.7.

[241] Evid. Code, § 1043.

[242] *E.E.O.C. v. County of San Benito* (N.D.Cal. 1993) 818 F.Supp. 289; *Soto v. City of Concord* (N.D.Cal. 1995) 162 F.R.D. 603; Pen. Code, § 832.7

[243] *Garrett v. Young* (2003) 109 Cal.App.4th 1393 [1 Cal.Rptr.3d 134].

[244] *Pettus v. Cole* (1996) 49 Cal.App.4th 402, 442-43 [57 Cal.Rptr.2d 46, 73-74], as mod. on den. of rehg., review den.

[245] *Shaddox v. Bertani* (2003) 110 Cal.App.4th 1406 [2 Cal.Rptr.3d 808], rehg. den.

[246] *Loder v. City of Glendale* (1997) 14 Cal.4th 846 [59 Cal.Rptr.2d 696], cert. den. 522 U.S. 807 [118 S.Ct. 44].

[247] *Leonel v. American Airlines, Inc.* (9th Cir. 2005) 400 F.3d 702, 709, opn. amended on den. of rehg. (9th Cir. 2005) 2005 WL 976985.

[248] *Leonel v. American Airlines, Inc.* (9th Cir. 2005) 400 F.3d 702, 708, opn. amended on den. of rehg. (9th Cir. 2005) 2005 WL 976985 [citing 42 U.S.C. § 12112(d)(Unconstitutional or Preempted, Proposed Legislation); Gov. Code, § 12940, subd. (d)].

[249] See, 42 U.S.C. § 12114(d)(1).

[250] Gov. Code, § 12926, subds. (i)(5) & (k)(6); *Loder v. City of Glendale* (1997) 14 Cal.4th 846, 865 [59 Cal.Rptr.2d 696], cert. den. 522 U.S. 807 [118 S.Ct. 44].

[251] See, EEOC's ADA Enforcement Guidance: Preemployment Disability Related Questions and Medical Examinations (Oct. 1995) p. 14 [cited with approval in *Leonel v. American Airlines, Inc.* (9th Cir. 2005) 400 F.3d at 711, opn. amended on den. of rehg. (9th Cir. 2005) 2005 WL 976985].

[252] See, EEOC's ADA Enforcement Guidance: Preemployment Disability Related Questions and Medical Examinations (Oct. 1995) p. 9.

[253] *Edgerton v. State Personnel Bd.* (2000) 83 Cal.App.4th 1350 [100 Cal.Rptr.2d 491], rehg. & review den.

[254] *Skinner v. Railway Labor Executives' Ass'n* (1989) 489 U.S. 602 [109 S.Ct. 1402].

[255] *Loder v. City of Glendale* (1997) 14 Cal.4th 846 [59 Cal.Rptr.2d 696], cert. den. 522 U.S. 807 [118 S.Ct. 44].

[256] *United Teachers of New Orleans v. Orleans Parish School Bd. through Holmes* (5th Cir. 1998) 142 F.3d 853.

[257] *National Treasury Employees Union v. Von Raab* (5th Cir. 1989) 876 F.2d 376.

[258] *Skinner v. Railway Labor Executives' Ass'n* (1989) 489 U.S. 602 [109 S.Ct. 1402].

[259] *Connelly v. Newman* (N.D.Cal., 1990) 753 F.Supp. 293.

[260] *Smith v. Fresno Irrigation Dist*. (1999) 72 Cal.App.4th 147 [84 Cal.Rptr.2d 775], rehg. den. and review den.

[261] *American Federation of Labor v. Unemployment Ins. Appeals Bd*. (1994) 23 Cal.App.4th 51 [28 Cal.Rptr.2d 210], as mod. on den. of rehg.

[262] *American Federation of Government Employees, AFL-CIO v. Roberts* (9th Cir. 1993) 9 F.3d 1464.

[263] *International Broth. of Teamsters, Chauffers, Western Conference of Teamsters v. Department of Transportation* (9th Cir. 1991) 932 F.2d 1292.

[264] *International Brotherhood of Electrical Workers, Local 1245 v. U.S. Nuclear Regulatory Commission* (9th Cir. 1992) 966 F.2d 521.

[265] *American Federation of Government Employees, Local 1533 v. Cheney* (N.D.Cal., 1990) 754 F.Supp. 1409, judg. affd. (9th Cir. 1991) 944 F.2d 503.

[266] *Luck v. Southern Pacific Transportation Co*. (1990) 218 Cal.App.3d 1 [267 Cal.Rptr. 618], cert. den. (1990) 498 U.S. 939 [111 S.Ct. 344].

[267] *American Federation of Government Employees, L-2110 v. Derwinski* (N.D.Cal., 1991) 777 F.Supp. 1493.

[268] *Semore v. Pool* (1990) 217 Cal.App.3d 1087 [266 Cal.Rptr. 280], review den.

[269] *Luck v. Southern Pacific Transportation Co.* (1990) 218 Cal.App.3d 1 [267 Cal.Rptr. 618], cert. den. (1990) 498 U.S. 939 [111 S.Ct. 344].

[270] *Kraslawsky v. Upper Deck Co.* (1997) 56 Cal.App.4th 179 [65 Cal.Rptr.2d 297].

[271] *Holliday v. City of Modesto* (1991) 229 Cal.App.3d 528 [280 Cal.Rptr. 206].

[272] 49 C.F.R. § 40.25.

[273] 49 C.F.R. § 40.25.

[274] 49 C.F.R. § 40.25(a).

[275] 49 C.F.R. § 40.25(b).

[276] 49 C.F.R. § 40.25(c).

[277] 49 C.F.R. § 40.25(d).

[278] 49 C.F.R. § 40.25(e).

[279] 49 C.F.R. § 40.25(f).

[280] 49 C.F.R. § 40.25(h).

[281] 49 C.F.R. § 40.25(g).

[282] 49 C.F.R. § 40.25(g).

[283] 49 C.F.R. § 40.25(i).

[284] 49 C.F.R. § 40.25(i).

[285] 49 C.F.R. § 40.25(j).

[286] 49 C.F.R. § 40.25(j).

[287] *Craig v. Municipal Court* (1979) 100 Cal.App.3d 69 [161 Cal.Rptr. 19].

[288] *Britt v. Superior Court* (1978) 20 Cal.3d 844 [143 Cal.Rptr. 695].

[289] *Board of Trustees v. Superior Court* (1981) 119 Cal.App.3d 516 [174 Cal.Rptr. 160]; see also *Pomona College v. Superior Court* (1996) 45 Cal.App.4th 1716 [53 Cal.Rptr.2d 662].

[290] *Miller v. Chico Unified School Dist.* (1979) 24 Cal.3d 703 [157 Cal.Rptr. 72].

[291] *Woodland Joint Unified School Dist. v. Commission of Professional Competence* (1992) 2 Cal.App.4th 1429 [4 Cal.Rptr.2d 227], review den.

[292] *Aguilar v. Johnson* (1988) 202 Cal.App.3d 241, 249 [247 Cal.Rptr. 909, 913].

[293] *Board of Trustees v. Superior Court* (1981) 119 Cal.App.3d 516 [174 Cal.Rptr. 160].

[294] *Brutsch v. City of Los Angeles* (1992) 3 Cal.App.4th 354 [4 Cal.Rptr.2d 456], review den.

[295] *Board of Trustees v. Superior Court* (1981) 119 Cal.App.3d 516 [174 Cal.Rptr. 160]; disapproved of on other grounds by *Williams v. Superior Ct.* (2017) 3 Cal.5th 531.

[296] *Brutsch v. City of Los Angeles* (1992) 3 Cal.App.4th 354 [4 Cal.Rptr.2d 456], review den.

[297] *Brutsch v. City of Los Angeles* (1992) 3 Cal.App.4th 354, 360 [4 Cal.Rptr.2d 456, 459], review den.

[298] *Pasadena Police Officers Association v. City of Pasadena* (1990) 51 Cal.3d 564 [273 Cal.Rptr. 584].

[299] Gov. Code, § 54957.7.

[300] Gov. Code, § 54957.

[301] 33 Ops.Cal.Atty.Gen. 32 (1959); 63 Ops.Cal.Atty.Gen. 153 (1980).

[302] *Bollinger v. San Diego Civil Service Com.* (1999) 71 Cal.App.4th 568, 574 [84 Cal.Rptr.2d 27]; see also *Fischer v. Los Angeles Unified School Dist.* (1999) 70 Cal.App.4th 87, 96-97 [82 Cal.Rptr.2d 452, 457-458], review den.

[303] *Kolter v. Commission on Professional Competence of the Los Angeles Unified School District* (2009) 170 Cal.App.4th 1346 [88 Cal.Rptr.3d 620], review den.

[304] *Kolter v. Commission on Professional Competence of the Los Angeles Unified School District* (2009) 170 Cal.App.4th 1346 [88 Cal.Rptr.3d 620], review den.

[305] *Furtado v. Sierra Community College* (1998) 68 Cal.App.4th 876 [80 Cal.Rptr.2d 589].

[306] *Fischer v. Los Angeles Unified School District* (1999) 70 Cal.App.4th 87 [82 Cal.Rptr.2d. 452], rehg. den. & review den.

[307] *Bollinger v. San Diego Civil Service Com*. (1999) 71 Cal.App.4th 568 [84 Cal.Rptr.2d 27].

[308] *Morrison v. Housing Authority of the City of Los Angeles Bd. of Comrs*. (2003) 107 Cal.App.4th 860 [132 Cal.Rptr.2d 453].

[309] *Moreno v. City of King* (2005) 127 Cal.App.4th 17 [25 Cal.Rptr.3d 29].

[310] 75 Ops.Cal.Atty.Gen. 51 (1992).

[311] *Gillespie v. San Francisco Public Library Commission* (1998) 67 Cal.App.4th 1165 [79 Cal.Rptr.2d 649].

[312] Gov. Code, §§ 6250 et seq.

[313] 5 U.S.C. § 552 et seq. (Proposed Legislation)

[314] *Cook v. Craig* (1976) 55 Cal.App.3d 773, 781 [127 Cal.Rptr. 712, 716].

[315] *State of California ex rel. Division of Industrial Safety v. Superior Court* (1974) 43 Cal.App.3d 778, 783 [117 Cal.Rptr. 726, 729]. See also, *Johnson v. Winter* (1982) 127 Cal.App.3d 435 [179 Cal.Rptr. 585].

[316] Gov. Code, § 6252, subd. (e); *Roberts v. City of Palmdale* (1993) 5 Cal.4th 363 [20 Cal.Rptr.2d 330].

[317] *Braun v. City of Taft* (1984) 154 Cal.App.3d 332, 340 [201 Cal.Rptr. 654, 658], citing *San Gabriel Tribune v. Superior Court* (1983) 143 Cal.App.3d 762, 774 [192 Cal.Rptr. 415].

[318] *City of San Jose et al. v. The Superior Court of Santa Clara County* (2014) 225 Cal.App.4th 75, 96 [169 Cal.Rptr.3d 840], review granted & opinion superseded by *City of San Jose v. S.C.* (2014) 173 Cal.Rptr.3d 46.

[319] *City of San Jose et al. v. The Superior Court of Santa Clara County* (2014) 225 Cal.App.4th 75, 96 [169 Cal.Rptr.3d 840], review granted & opinion superseded by *City of San Jose v. S.C.* (2014) 173 Cal.Rptr.3d 46.

[320] *City of San Jose v. S.C.* (2014) 173 Cal.Rptr.3d 46.

[321] *Black Panther Party v. Kehoe* (1974) 42 Cal.App.3d 645, 652 [117 Cal.Rptr. 106, 110].

[322] *Braun v. City of Taft* (1984) 154 Cal.App.3d at 342 [201 Cal.Rptr. 654, 659]; *San Gabriel Tribune v. Superior Court* (1983) 143 Cal.App.3d 762, 772-773, [192 Cal.Rptr. 415, 420-421].

[323] *Braun v. City of Taft* (1984) 154 Cal.App.3d 332, 340 [201 Cal.Rptr. 654, 662].

[324] *Rogers v. Superior Court* (1993) 19 Cal.App.4th 469 [23 Cal.Rptr.2d 412], as mod.

[325] *Versaci v. Superior Court (Palomar Community College District)* (2005) 127 Cal.App.4th 805 [26 Cal.Rptr.3d 92], rehg. & review den.

[326] *Braun v. City of Taft* (1984) 154 Cal.App.3d 332, 340 [201 Cal.Rptr. 654, 658].

[327] *Versaci v. Superior Court (Palomar Community College District)* (2005) 127 Cal.App.4th 805 [26 Cal.Rptr.3d 92], rehg. & review den.

[328] *International Federation of Professional and Technical Engineers, Local 21, AFL-CIO v. Superior Court* (2007) 42 Cal.4th 319 [64 Cal.Rptr.3d 693].

[329] *County of Los Angeles v. Superior Court* (1993) 18 Cal.App.4th 588 [22 Cal.Rptr.2d 409].

[330] *Marken v. Santa Monica-Malibu Unified School Dist.* (2012) 202 Cal.App.4th 1250 [136 Cal.Rptr.3d 395], review den.

[331] *Bakersfield City School District v. Superior Court* (2004) 118 Cal.App.4th 1041 [13 Cal.Rptr.3d 517].

[332] *BRV, Inc. v. Superior Court* (2006) 143 Cal.App.4th 742.

[333] *Caldecott v. Superior Court* (2015) 243 Cal.App.4th 212.

[334] *Petaluma v. Superior Court of Sonoma County* (2016) 248 Cal.App.4th 1023

[335] *City of Hemet v. Superior Court* (1995) 37 Cal.App.4th 1411 [44 Cal.Rptr.2d 532], review den.

[336] *Belth v. Garamendi* (1991) 232 Cal.App.3d 896 [283 Cal.Rptr. 829].

[337] *Copley Press, Inc. v. Superior Court* (2006) 39 Cal.4th 1272 [48 Cal.Rptr.3d 183].

[338] *Long Beach Police Officers Association v. City of Long Beach* (2014) 59 Cal.4th 59 [172 Cal.Rptr.3d 56].

[339] *Pasadena Police Officers Association v. Superior Court* (2015) --- Cal.App.4th --- [192 Cal.Rptr.3d 486].

[340] Office of the Attorney General Opinion No. 12-401; --- Ops. Cal. Atty. Gen. --- (October 13, 2015).

[341] *People v. Superior Court (Johnson)* (2015) 61 Cal.4th 696.

[342] *Brady v. Maryland* (1963) 373 U.S. 83.

[343] *Pitchess v. Superior Court* (1974) 11 Cal.3d 531.

[344] *Fredericks v. Superior Court of San Diego County* (2015) 233 Cal.App.4th 209; disapproved of on other grounds by *Nat'l Laws. Guild , San Francisco Bay Area Chapter v. City of Hayward* (2020) 9 Cal. 5th 488.

[345] *Association for Los Angeles Deputy Sheriffs v. Los Angeles Times Communication LLC* (2015) 239 Cal.App.4th 808.

[346] *Detroit Edison Co. v. N.L.R.B.* (1979) 440 U.S. 301 [99 S.Ct. 1123].

[347] *N.L.R.B. v. New England Newspapers, Inc*. (1st Cir. 1988) 856 F.2d 409, 413.

[348] *County of Los Angeles v. Los Angeles County Employee Relations Com.* (2013) 56 Cal.4th 905 [157 Cal.Rptr.3d 481].

[349] *Los Angeles Unified School District* (2015) PERB Decision No. 2438-E, 40 PERC ¶ 26.

[350] *Teamsters, Local 350 v. City of Los Altos* (2007) PERB Dec. No. 1891-M [31 PERC ¶ 74].

[351] Gov. Code, § 7285.1(a).

[352] Gov. Code, § 7285.2(a)(1).

[353] See Gov. Code, §§ 7285.1(b) and 7285.2(b).

[354] See Gov. Code, §§ 7285.1(b) and 7285.2(b).

[355] See Gov. Code, § 7285.1(b).

[356] See Gov. Code, § 7285.1(c)

[357] See Gov. Code, § 7285.1(c).

[358] See Gov. Code, § 7285.2(b).

[359] Gov. Code, § 7285.2(a)(1).

[360] Gov. Code, § 7285.2(a)(2).

[361] Labor Code, § 90.2(a)(1).

[362] Labor Code, § 90.2(a)(1).

[363] Labor Code, § 90.2(a)(1).

[364] Labor Code, § 90.2(a)(1)(A)-(D).

[365] Labor Code, § 90.2(a)(2).

[366] Labor Code, § 90.2(a)(3).

[367] Labor Code, § 90.2(b).

[368] Labor Code, § 90.2(b).

[369] Labor Code, § 90.2(b).

[370] Labor Code, § 90.2(b)(1)(A)-(D).

[371] Labor Code, § 90.2(c).

[372] Labor Code, § 90.2(c).

[373] *Williams v. Superior Court* (2017) 3 Cal.5th 531, 552.

[374] *Board of Trustees v. Superior Court* (1981) 119 Cal.App.3d 516, 525 [174 Cal.Rptr. 160, 164] ; disapproved of on other grounds by *Williams v. Superior Ct.* (2017) 3 Cal.5th 531.

[375] *Harding Lawson Associates v. Superior Court* (1992) 10 Cal.App.4th 7 [12 Cal.Rptr.2d 538, 539]; disapproved of on other grounds by *Williams v. Superior Ct.* (2017) 3 Cal.5th 531..

[376] *El Dorado Savings & Loan Assn. v. Superior Court* (1987) 190 Cal.App.3d 342 [235 Cal.Rptr. 303]; disapproved of on other grounds by *Williams v. Superior Ct.* (2017) 3 Cal.5th 531..

[377] *City of San Diego v. Superior Court* (1981) 136 Cal.App.3d 236 [186 Cal.Rptr.112].

[378] Fed. Rules Civ.Proc., rules 16(b)(5)(6), 26(a)(1)(B), (b)(1)(B). (b)(5)(B), (f)(3)(4), 33(d), 34(a)(b), 37(f), 45(a)(1)(C)(D), (a)(2)(C), (b)(2)(A) & (d)(1)(B)(C)(D); 28 U.S.C.

[379] *Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2003) 220 F.R.D. 212, 219-220; but see *In re Electric Machinery Enterprises, Inc.* (2009) 416 B.R. 801, 874 (where, in 11th Circuit, the determination of whether to impose spoliation sanctions is "informed by" state law and, thus, the court did not impose spoliation sanctions as there was no duty to preserve under state law at the time the actions were taken).

[380] *University of Pennsylvania v. E.E.O.C.* (1990) 493 U.S. 182 [110 S.Ct. 577].

[381] Code Civ. Proc., § 1985.4.

[382] *Lantz v. Superior Court* (1994) 28 Cal.App.4th 1839 [34 Cal.Rptr.2d 358].

[383] *Pitchess v. Superior Court* (1974) 11 Cal.3d 531 [113 Cal.Rptr. 897], superceded by statute (2011) 2011 WL 3681565.

[384] *City of Redding v. Municipal Court* (1988) 200 Cal.App.3d 1181, 1186-87 [246 Cal.Rptr. 417, 421], review den.

[385] *Jalilie v. Superior Court* (1988) 195 Cal.App.3d 487 [240 Cal.Rptr. 662], review den.

[386] *City of San Jose v. Superior Court* (1993) 5 Cal.4th 47, 50, 53 [19 Cal.Rptr.2d 73, 75], review den.

[387] *People v. Mooc* (2001) 26 Cal.4th 1216 1216 [114 Cal.Rptr.2d 482], as mod.

[388] 66 Ops.Cal.Atty.Gen. 128 (1983).

[389] *Welsh v. City and County of San Francisco* (N.D. Cal. 1995) 887 F.Supp. 1293.

[390] *Michael v. Gates* (1995) 38 Cal.App.4th 737 [45 Cal.Rptr.2d 163].

[391] *Commission on Peace Officer Standards & Training v. Superior Court* (2007) 42 Cal.4th 278 [64 Cal.Rptr.3d 661]; *International Federation of Professional and Technical Engineers Local 21, AFL-CIO v. Superior Court* (2007) 42 Cal.4th 319 [64 Cal.Rptr.3d 693].

[392] *International Federation of Professional and Technical Engineers Local 21, AFL-CIO v. Superior Court* (2007) 42 Cal.4th 319 [64 Cal.Rptr.3d 693].

[393] *Ortega v. O'Connor* (9th Cir 1998) 146 F.3d 1149.

[394] *O'Connor v. Ortega* (1987) 480 U.S. 709 [107 S.Ct. 1492], affd. (1998) 146 F.3d 149.

[395] *O'Connor v. Ortega* (1987) 480 U.S. 709, 725–726 [107 S.Ct. 1492, 94 L.Ed.2d 714], affd. (1998) 146 F.3d 149.

[396] *Ortega v. O'Connor* (9th Cir. 1998) 146 F.3d 1149, 1166 .

[397] *City of Ontario, Cal. v. Quon* (2010) 560 U.S. 746 [130 S.Ct. 2619, 177 L.Ed.2d 216], distinguished by (2011) 770 F.Supp.2d 1042.

[398] *Crispin v. Christian Audigier, Inc.* (C.D. Cal. 2010) 717 F.Supp.2d 965.

[399] *Riley v. California* (2014) 134 S.Ct. 2473.

[400] *Williams v. Superior Court* (2017) 3 Cal.5th 531 [220 Cal.Rptr.3d 472, 398 P.3d 69].

[401] *Williams v. Superior Court* (2017) 3 Cal.5th 531, 556 [220 Cal.Rptr.3d 472, 398 P.3d 69].

[402] Gov. Code, § 3309.

[403] *Los Angeles Police Protective League v. Gates* (9th Cir. 1993) 995 F.2d 1469.

[404] *O'Connor v. Ortega* (1987) 480 U.S. 709 [107 S.Ct. 1492, 94 L.Ed.2d 714], affd. *Ortega v. O'Connor* (9th Cir. 1998) 146 F.3d 1149.

[405] *Finkelstein v. State Personnel Bd.* (1990) 218 Cal.App.3d 264 [267 Cal.Rptr. 133], review den.

[406] *Katz v. United States* (1967) 389 U.S. 347 [88 S.Ct. 507], superceded by statute (9th Cir. 1991) 946 F.2d 1450, criticized (1996) 51 Cal.App.4th 1468 [59 Cal.Rptr.2d 634].

[407] *Haynes v. Office of Atty Gen. Phill Kline* (2003) 298 F.Supp.2d 1154.

[408] *Ortega v. O'Connor* (9th Cir. 1985) 764 F.2d 703, revd. (1987) 480 U.S. 709 [107 S.Ct. 1492].

[409] *Ortega v. O'Connor* (9th Cir. 1985) 764 F.2d 703, revd. (1987) 480 U.S. 709, 717, 724 [107 S.Ct. 1492].

[410] 18 U.S.C. §§ 2510-2520. (Unconstitutional or Preempted, Proposed Legislation)

[411] 18 U.S.C § 2511(1). **(Unconstitutional or Preempted, Proposed Legislation)**

[412] *Hutton v. Woodall* (D. Colorado 2014) 70 F.Supp.3d 1235, 1240.

[413] 18 U.S.C. § 2701(a)(1).

[414] *Quon v. Arch Wireless Operating Co., Inc.* (9th Cir. 2008) 529 F.3d 892, 900, revd. & remanded (2010) 130 S.Ct. 2619, distinguished by (2011)191 Cal.App.4th 1047 [119 Cal.Rptr.3d 878] (provision cited for still good law).

[415] *Quon v. Arch Wireless Operating Co., Inc.* (9th Cir. 2008) 529 F.3d 892, revd. & remanded (2010) 130 S.Ct. 2619, distinguished by (2011) 191 Cal.App.4th 1047 [119 Cal.Rptr.3d 878] (provision cited for still good law).

[416] *City of Ontario, Cal. v. Quon* (2010) 560 U.S. 746 [130 S.Ct. 2619], distinguished by (2011) 770 F.Supp.2d 1042.

[417] *Watkins v. L. M. Berry & Co.* (11th Cir. 1983) 704 F.2d 577.

[418] *Briggs v. American Air Filter Co., Inc.* (5th Cir. 1980) 630 F.2d 414.

[419] *Epps v. St. Mary's Hospital of Athens, Inc.* (11th Cir. 1986) 802 F.2d 412, rehg. den. 807 F.2d 999.

[420] *Bohach v. City of Reno* (D. Nev. 1996) 932 F.Supp. 1232.

[421] *U.S. v. Simons* (E.D.Va. 1998) 29 F.Supp.2d 324, cert. den. (2001) 534 U.S. 930 [122 S.Ct. 292].

[422] *United States v. Ziegler* (9th Cir. 2007) 474 F.3d 1184, cert. den. (2008) 552 U.S. 1105 [128 S.Ct. 879].

[423] *Wasson v. Sonoma County Jr. College Dist*. (N.D.Cal. 1997) 4 F.Supp.2d 893, 905-907, affd. on other grounds (9th Cir. 2000) 203 F.3d 659.

[424] *U.S. v. Angevine* (10th Cir. 2002) 281 F.3d 1130, cert. den. 537 U.S. 845 [123 S.Ct. 182].

[425] *Deal v. Spears* (8th Cir. 1992) 980 F.2d 1153.

[426] *Biby v. Board of Regents of University of Nebraska at Lincoln* (8th Cir. 2005) 419 F.3d 845.

[427] *Clauson v. Superior Court* (1998) 67 Cal.App.4th 1253 [79 Cal.Rptr.2d 747].

[428] *McVeigh v. Cohen* (D.D.C. 1998) 983 F.Supp. 215.

[429] Pen. Code, Cal. Penal Code § 502, subd. (a).

[430] *People v. Childs* (2013) 220 Cal.App.4th 1079 [164 Cal.Rptr.3d 287].

[431] *People v. Childs* (2013) 220 Cal.App.4th 1079 [164 Cal.Rptr.3d 287].

[432] *People v. Childs* (2013) 220 Cal.App.4th 1079 [164 Cal.Rptr.3d 287].

[433] *People v. Childs* (2013) 220 Cal.App.4th 1079 [164 Cal.Rptr.3d 287].

[434] Pen. Code, §§ 630 et seq.

[435] Pen. Code, § 631.

[436] Pen. Code, § 632.

[437] *Warden v. Kahn* (1979) 99 Cal.App.3d 805 [160 Cal.Rptr. 471].

[438] Pen. Code, § 637.

[439] *TBG Ins. Services Corp. v. Superior Court* (2002) 96 Cal.App.4th 443 [117 Cal.Rptr.2d 155], rehg. & review den.

[440] Lab. Codem § 980, sub. (a).

[441] See Calif. Penal Code §§ 632 and 633.

[442] *Telish v. California State Personnel Bd.* (2015) 234 Cal.App.4th 1479.

[443] (Pen. Code, §§ 1546.1(a)(1)-(3).)

[444] *Intel Corp. v. Hamidi* (2003) 30 Cal.4th 1342 [1 Cal.Rptr.3d 32].

[445] *Purple Communications, Inc. and Communications Workers of America, ALF-CIO*, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand *Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision*, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[446] *Purple Communications, Inc. and Communications Workers of America, ALF-CIO*, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand *Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision*, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[447] *Purple Communications, Inc. and Communications Workers of America, ALF-CIO*, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand *Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision*, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[448] *Holmes v. Petrovich Development Company* (2011) 191 Cal.App.4th 1047 [119 Cal.Rptr.3d 878].

[449] *In re Reserve Fund Securities and Derivative Litigation* (S.D.N.Y. 2011) 275 F.R.D. 154.

[450] *In re Reserve Fund Securities and Derivative Litigation* (S.D.N.Y. 2011) 275 F.R.D. 154.

[451] *In re Asia Global Crossing, Ltd.* (Bankr. S.D.N.Y. 2005) 322 BR 247, 257.

[452] *In re Reserve Fund Securities and Derivative Litigation* (S.D.N.Y. 2011) 275 F.R.D. 154.

[453] *In re Reserve Fund Securities and Derivative Litigation* (S.D.N.Y. 2011) 275 F.R.D. 154.

[454] *In re Reserve Fund Securities and Derivative Litigation* (S.D.N.Y. 2011) 275 F.R.D. 154.

[455] *Hernandez v. Hillsides, Inc.* (2009) 47 Cal.4th 272 [97 Cal.Rptr.3d 274], distinguished (2011) 775 F.Supp.2d 1176.

[456] *Sacramento County Deputy Sheriffs' Assn. v. County of Sacramento* (1996) 51 Cal.App.4th 1468 [59 Cal.Rptr.2d 834], cert. den. (1997) 520 U.S. 1124 [117 S.Ct. 1265].

[457] *Trujillo v. City of Ontario* (C.D. Cal. 2006) 428 F.Supp.2d 1094, distinguished (2009) 47 Cal.4th 272 [97 Cal.Rptr.3d 274].

[458] *Blanco v. County of Kings* (E.D.Calif. 2015) 142 F.Supp.3d 986, fn. 6.

[459] *Blanco v. County of Kings* (E.D.Calif. 2015) 142 F.Supp.3d 986, fn. 6.

[460] *Richardson-Tunnell v. School Ins. Program for Employees (SIPE)* (2007) 157 Cal.App.4th 1056 [69 Cal Rptr.3d 176], rehg. & review den (2008).

[461] *Sanders v. American Broadcasting Companies, Inc.* (1999) 20 Cal.4th 907 [85 Cal.Rptr.2d 909].

[462] Ops.Cal Atty Gen No. 12-1101 (February 14, 2014) [2014 WL 587948].

[463] *Rio Hondo Community College District* (2013) PERB Decision No. 2313E.

[464] *Rio Hondo Community College District* (2013) PERB Decision No. 2313E.

[465] *Whole Foods Market, Inc.* (December 24, 2015) 363 NLRB No.87.

[466] Pen. Code, § 637.7, subd. (a).

[467] Pen. Code, § 637.7, subd. (b).

[468] Pen. Code, § 637.7, subd. (c).

[469] *United States v. Jones* (2012) 132 S.Ct. 945.

[470] "Off-highway Vehicle (OHV) Telematics Market: Global Industry Analysis and Opportunity Assessment, 2016-2026," PR Newswire (June 21, 2016), http://www.prnewswire.com/news-releases/off-highway-vehicle-ohv-telematics-market-global-industry-analysis-and-opportunity-assessment-20162026-300288141.html.

[471] "Telematics", *Encyclopedia*, PCMag.com, http://www.pcmag.com/encyclopedia_term/0,1237,t=telematics&i=52693,00.asp.

[472] "Telematics", *Encyclopedia*, PCMag.com, http://www.pcmag.com/encyclopedia_term/0,1237,t=telematics&i=52693,00.asp.

[473] "Vehicle Telematics: Risk Management at Every Turn" (Risk Management Magazine), The National Law Review (June 12, 2010), http://www.natlawreview.com/article/vehicle-telematics-risk-management-every-turn.

[474] Pellitta, F., "The Use of Telematics in the Preventative Maintenance Aspects of Fleets," Telematics.com (April 13, 2015), http://www.telematics.com/the-use-of-telematics-in-the-preventative-maintenance-aspects-of-fleets/.

[475] *Building Material & Construction Teamsters' Union v. Farrell* (1986) 41 Cal.3d 651[224 Cal.Rptr. 688]; Gov. Code, §§ 3500-3510.

[476] *Valencia v. County of Sonoma* (2007) 158 Cal.App.4th 644 [69 Cal.Rptr.3d 881].

[477] Pen. Code, §637.7, subd. (a).

[478] Biometrics Glossary prepared by The National Science and Technology Council (NSTC), Subcom. On Biometrics and Identity Management (Sep. 14, 2006) http://www.biometrics.gov/Documents/glossary.pdf.

[479] Biometrics Glossary prepared by The National Science and Technology Council (NSTC), Subcom. On Biometrics and Identity Management (Sep. 14, 2006) <http://www.biometrics.gov/Documents/glossary.pdf.

[480] Maher, *Big Employer Is Watching* (Nov. 4, 2003) Wall Street Journal Online http://webreprints.djreprints.com /86195052181.html [as of Jul. 5, 2011].

[481] Jain, A., Hong, L. & Pankanti, S. (2000) "Biometric Identification", *Communications of the* ACM, 43(2), p. 91-98, http://www.andrew.cmu.edu/course/67-302/BiometricsACM.pdf.

[482] *Doe v. XYC Corp.* (2005) 382 N.J. Super. 122 [887 A.2d 1156].

[483] *DFEH (Plunkett) v. Insurance America Sales Agency* (1988) FEHC Dec. No. 88-07, Case No. FEP84-85 L2-0183 L-36370 88-07.

[484] *DFEH (Plunkett) v. v. Insurance America Sales Agency* (1988) FEHC Dec. No. 88-07, Case No. FEP84-85 L2-0183 L-36370 88-07.

[485] *DFEH (Goehring) v. City of Simi Valley* (1983) FEHC Dec. No. 83-21, Case No. FEP80-81 L7-0297 L-27332 83-21.

[486] *Miller v. Department of Corrections* (2005) 36 Cal.4th 446 [30 Cal.Rptr.3d 797].

[487] *Miller v. Department of Corrections* (2005) 36 Cal.4th 446 [30 Cal.Rptr.3d 797].

[488] *Proksel v. Gattis* (1996) 41 Cal.App.4th 1626 [49 Cal.Rptr.2d 322].

[489] *Samson v. Allstate Insurance Co.* (N.D.Cal. 1996) 949 F.Supp. 748.

[490] *Hardage v. CBS Broadcasting, Inc*. (9th Cir. 2005) 427 F.3d 1177, 1183-84, as amended on denial of rehg. (9th Cir. 2006) 433 F.3d 672, cert. den. (2006) 549 U.S. 812 [127 S.Ct. 55].

[491] *Barbee v. Household Automotive Finance Corp*. (2003) 113 Cal.App.4th 525 [6 Cal.Rptr.3d 406].

[492] *Barbee v. Household Automotive Finance Corp*. (2003) 113 Cal.App.4th 525, 531-32 [6 Cal.Rptr.3d 406, 410-411].

[493] *Crosier v. United Parcel Service, Inc.* (1983) 150 Cal.App.3d 1132 [198 Cal.Rptr. 361]], overruled on other grounds (1989) 48 Cal.3d 973 [258 Cal.Rptr. 590] and disapproved of by *Foley v. Interactive Data Corp.* (1988) 47 Cal.3d 654, 688 [254 Cal.Rptr. 211, 230-31].

[494] *Shuman v. City of Philadelphia* (D.C. Pa. 1979) 470 F.Supp. 449, 459.

[495] *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459, cert. den. (1984) 469 U.S. 979 [105 S.Ct. 380, 383] and app. after remand (1986) 802 F.2d 1131, disagreed with (E.D. Mich. 2000) 81 F.Supp.2d 814.

[496] *Shawgo v. Spradlin* (5th Cir. 1983) 701 F.2d 470, 483, cert. den. 464 U.S.965 [104 S.Ct. 404].

[497] *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459] and app. after remand (1986) 802 F.2d 1131, disagreed with (E.D. Mich. 2000) 81 F.Supp.2d 814.

[498] *Anderson v. State Personnel Bd.* (1987) 194 Cal.App.3d 761 [239 Cal.Rptr. 824], review den.

[499] *Fleisher v. City of Signal Hill* (9th Cir. 1987) 829 F.2d 1491, cert. den. (1988) 485 U.S. 961 [108 S.Ct.1225].

[500] *Fugate v. Phoenix Civil Service Bd.* (9th Cir. 1986) 791 F.2d 736.

[501] *Bailey v. City of National City* (1991) 226 Cal.App.3d 1319 [277 Cal.Rptr. 427], review & cert. den. 502 U.S. 859 [112 S.Ct.176].

[502] *Vielehr v. State Personnel Board* (1973) 32 Cal.App.3d 187 [107 Cal.Rptr. 852].

[503] *Dible v. City of Chandler*, (9th Cir. 2008) 515 F.3d 918, 926.

[504] *San Diego Unified School Dist. v. Commission on Professional Competence (Lampedus)* (2011) 194 Cal.App.4th 1454 [124 Cal.Rptr.3d 320].

[505] See *American Medical Response of Connecticut, Inc*. NLRB Case No. 34-CA-12576, *Lee Enterprises, Inc., d/b/a Arizona Daily Star*, NLRB Case No. 28-CA-23267, *Hispanics United of Buffalo*, NLRB Case No. 03-CA-027872, *Knauz BMW*, NLRB Case No. 13, CA-046452.

[506] Purple Communications, Inc. and Communications Workers of America, ALF-CIO, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[507] Purple Communications, Inc. and Communications Workers of America, ALF-CIO, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[508] Purple Communications, Inc. and Communications Workers of America, ALF-CIO, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[509] Purple Communications, Inc. and Communications Workers of America, ALF-CIO, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (December 11, 2014) and on remand Purple Communications, Inc. and Communications Workers of America, AFL-CIO Supplemental Decision, Cases 21-CA-095151, 21-RC-091531, and 21-RC-091584 (March 16, 2015).

[510] NLRB, Office of the General Counsel Memorandum OM 11-74, Report of the Acting General Counsel Concerning Social Media Cases August 18, 2011, found at https://www.nlrb.gov/reports-guidance/general-counsel-memos.

[511] NLRB, Complaint issued against New York nonprofit for unlawfully discharging employees following Facebook posts (Jun. 28, 2011), https://www.nlrb.gov/news-outreach/news-story/complaint-issued-against-new-york-nonprofit-unlawfully-discharging; see also https://www.nlrb.gov/news-outreach/news-story/administrative-law-judge-finds-new-york-nonprofit-unlawfully-discharged.

[512] NLRB, Chicago car dealership wrongfully discharged employee for Facebook posts, complaint alleges (May 24, 2011), http://www.nlrb.gov/news/chicago-car-dealership-wrongfully-discharged-employee-facebook-posts-complaint-alleges.

[513] *NLRB, Office of the General Counsel, Advice Memorandum* (*Lee Enterprises, Inc. d/b/a Arizona Daily Star*, NLRB Case No. 28-CA-23267) (Apr. 21, 2011), https://www.nlrb.gov/cases-decisions/advice-memos?issuance_date=2011&page=2.

[514] *Butler Medical Transport, LLC and Michael Rice and William Lewis Norvell*, Case Nos. 5-CA-97810, 5-CA-94981, and 5-CA-97854 (Sept. 4, 2013).

[515] *Butler Medical Transport, LLC and Michael Rice and William Lewis Norvell*, Case Nos. 5-CA-97810, 5-CA-94981, and 5-CA-97854 (Sept. 4, 2013).

[516] *Butler Medical Transport, LLC and Michael Rice and William Lewis Norvell*, Case Nos. 5-CA-97810, 5-CA-94981, and 5-CA-97854 (Sept. 4, 2013).

[517] NLRB, Office of the General Counsel, Memorandum GC 11-11, Mandatory Submissions to Advice (Apr. 12, 2011) section A.9, http://www.nlrb.gov/reports-guidance/general-counsel-memos.

[518] NLRB, Office of the General Counsel Memorandum OM 12-59, Report of the Acting General Counsel concerning social media cases (May 30, 2012), https://www.nlrb.gov/reports-guidance/general-counsel-memos. See also NLRB, Office of the General Counsel Memorandum GC 15-04, Report of the General Counsel concerning Employer Rules (March 18, 2015), http://www.nlrb.gov/reports-guidance/general-counsel-memos.

[519] NLRB, Office of the General Counsel Memorandum GC 15-04, Report of the General Counsel concerning Employer Rules (March 18, 2015), http://www.nlrb.gov/reports-guidance/general-counsel-memos.

[520] *Price Edwards & Company* (May 7, 2013) 2013 WL 4648481.

[521] *Price Edwards & Company* (May 7, 2013) 2013 WL 4648481.

[522] *California Institute of Technology Jet Propulsion Laboratory* (March 12, 2014) 360 NLRB No. 63.

[523] *MUSE School v. Trudy Perry*, NLRB Case No. 31-CA-108671.

[524] *Pickering v. Board of Ed. of Township High School Dist. 205, Will County, Ill.* (1968) 391 U.S. 563, 568 [88 S.Ct. 1731].

[525] *Cohen v. California* (1971) 403 U.S. 15 [91 S.Ct. 1780], rehg. den. by 404 U.S. 876 [92 S.Ct. 26].

[526] *Demers v. Austin* (9th Cir. 2014) 746 F.3d 402, 406.

[527] *Demers v. Austin* (9th Cir. 2014) 746 F.3d 402, 412.

[528] *Pickering v. Board of Educ. of Township High School Dist. 205, Will County, Ill.* (1968) 391 U.S. 563, 568 [88 S.Ct. 1731].

[529] *Connick v. Myers* (1983) 461 U.S. 138 [103 S.Ct. 1684, 75 L.Ed.2d 708].

[530] *Garcetti v. Ceballos* (2006) 547 U.S. 410 [126 S.Ct. 1951, 164 L.Ed.2d 689].

[531] *Pickering v. Board of Educ. of Township High School Dist. 205, Will County, Ill.* (1968) 391 U.S. 563, 568 [88 S.Ct. 1731]; *Connick v. Myers* (1983) 461 U.S. 138, 149 [103 S.Ct. 1684]; *Garcetti v. Ceballos* (2006) 547 U.S. 410, 421-422 [126 S.Ct. 1951].

[532] *Demers v. Austin* (9th Cir. 2014) 746 F.3d 402, 406.

[533] *Dahlia v. Rodriguez* (9th Cir. 2013) 735 F.3d 1060, cert den. (2014) 134 S.Ct. 1283.

[534] *Ellins v. City of Sierra Madre* (2013) 710 F.3d 1049.

[535] *Johnson v. Poway Unified School Dist*. (9th Cir. 2011) 658 F.3d 954, cert. den. (2012) 132 S.Ct. 1807.

[536] *Borough of Duryea v. Guarnieri* (2011) 564 U.S. 379 [131S.Ct. 2488].

[537] 29 U.S.C. § 215(a)(3). **(Proposed Legislation)**

[538] *Kasten v. Saint-Gobain Performance Plastics Corp.* (2011) 563 U.S. 1 [131 S.Ct. 1325], on remand to (7th Cir. 2011) 424 Fed.Appx. 564, opinion after remand (7th Cir. 2012) 703 F.3d 966.

[539] *Kasten v. Saint-Gobain Performance Plastics Corp.* (2011) 563 U.S. 1 [131 S.Ct. 1325], on remand to (7th Cir. 2011) 424 Fed.Appx. 564, opinion after remand (7th Cir. 2012) 703 F.3d 966.

[540] *Morse v. JP Morgan Chase & Co.* (M.D. Fla. 2011) Slip Opinion filed 6/24/11, Case No. 8:11-cv-00779-JDW-EAJ (http://www.michiganemploymentlawadvisor.com/retaliation/does-an-employer-violate-the-flsas-anti-retaliation-provision-for-firing-employee-for-facebook-posti/).

[541] *Morse v. JP Morgan Chase & Co.* (M.D. Fla. 2011) Slip Opinion filed 6/24/11, Case No. 8:11-cv-00779-JDW-EAJ (http://www.michiganemploymentlawadvisor.com/retaliation/does-an-employer-violate-the-flsas-anti-retaliation-provision-for-firing-employee-for-facebook-posti/).

[542] *Morse v. JP Morgan Chase & Co.* (M.D. Fla. 2011) Slip Opinion filed 6/24/11, Case No. 8:11-cv-00779-JDW-EAJ (http://www.michiganemploymentlawadvisor.com/retaliation/does-an-employer-violate-the-flsas-anti-retaliation-provision-for-firing-employee-for-facebook-posti/).

[543] *Emerson v. J.F. Shea Co.* (1978) 76 Cal.App.3d 579 [143 Cal.Rptr. 170].

[544] *Moreno v. Hanford Sentinel, Inc.* (2009) 172 Cal.App.4th 1125 [91 Cal.Rptr.3d 858], as mod. (Apr 30, 2009).

[545] *Lorenzana v. Superior Court* (1973) 9 Cal.3d [108 Cal.Rptr. 585, n 13]; *Noble v. Sears, Roebuck & Co*. (1973) 33 Cal.App.3d 654 [109 Cal.Rptr. 269].

[546] *Ehling v. Monmouth-Ocean Hosp. Service Corp*. (2013) 961 F.Supp.2d 659.

[547] Lab. Code, § 980, subd. (b).

[548] Lab. Code, § 980, sub. (c).

[549] Lab. Code, § 96, subd. (k).

[550] *Barbee v. Household Automotive Finance Corp*. (2003) 113 Cal.App.4th 525 [6 Cal.Rptr.3d 406].

[551] *Grinzi v. San Diego Hospice Corp.* (2004) 120 Cal.App.4th 72 [14 Cal.Rptr.3d 893], rehg. den.

[552] 83 Cal. Op. Att'y Gen. 226 (2000).

[553] Gov. Code, § 1126; *Long Beach Police Officers Assn. v. City of Long Beach* (1988) 46 Cal.3d 736 [250 Cal.Rptr. 869].

[554] *Long Beach Police officers Assn. v. City of Long Beach* (1988) 46 Cal.3d 736 [250 Cal.Rptr. 869, 759 P.2d 504].

[555] Pen. Code, § 70, subd. (e).

[556] Lab. Code, § 6404.5.

[557] Lab. Code, § 6404.5.

[558] 74 Cal. Op. Att'y Gen. 211 (1991).

[559] *County of Fresno v. Fair Employment & Housing Com.* (1991) 226 Cal.App.3d 1541 [277 Cal.Rptr. 557], rehg. & review den.

[560] *Vickers v. Veterans Admin.* (D.C. Wash. 1982) 549 F.Supp. 85, abrogation recognized (4th Cir. 1994) 14 F.3d 203.

[561] *Eureka Teachers Association v. Eureka City School District* (1992) PERB Dec. No. 955-E [16 PERC ¶ 23168].

[562] 42 U.S.C. § 12102(2)(C).

[563] *See Jespersen v. Harrah's Operating Co., Inc.* (9th Cir. 2006) 444 F.3d 1104, 1110 [employers may apply sex-differentiated appearance and grooming policies].

[564] DFEH, Transgender Rights in the Workplace (November 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/11/DFEH_E04P-ENG-2017Nov.pdf.

[565] DFEH, Transgender Rights in the Workplace (November 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/11/DFEH_E04P-ENG-2017Nov.pdf.

[566] *Kelley v. Johnson* (1976) 425 U.S. 238 [96 S.Ct. 1440].

[567] *Kennedy v. District of Columbia* (1994) 654 A.2d 847.

[568] *International Assn. of Fire Fighters Local 55 v. City of San Leandro* (1986) 181 Cal.App.3d 179 [226 Cal.Rptr. 238], rehg & review den.

LCW CCD Workbook Order Form

BROWN ACT/PUBLIC RECORDS ACT	QTY	COST	TOTAL
Public Meeting Law (the Brown Act) and the Public Records Act for Community College Districts		$55	
CONFLICTS OF INTEREST AND ETHICS			
Conflicts of Interest, Ethics and Open Government		$75	
DISABILITY AND OCCUPATIONAL SAFETY			
The Disability Interactive Process for Community Colleges		$75	
Managing Employee Injuries, Disability and Occupational Safety		$75	
DIVERSITY			
Diversity in Community College District Employment: Effective and Lawful EEO Hiring and Succession Planning		$75	
EDUCATION ADMINISTRATION ISSUES			
Frequently Used Education Code and Title 5 Sections for Community College Districts		$55	
EMPLOYMENT RELATIONS			
An Employment Relations Primer for CCD Administrators and Supervisors		$75	
Disaster Service Workers – If You Call Them, Will They Come?		$55	
Human Resources Academy I for CCDs		$55	
Human Resources Academy II for CCDs		$55	
Reductions in Staffing		$75	
Temporary Employees of a CCD		$75	
Terminating the Employment Relationship		$55	
EVALUATION AND DISCIPLINE			
Academic and Classified Evaluation and Discipline		$75	
FAIR LABOR STANDARDS ACT (FLSA)			
FLSA Fundamentals for School Districts and Community Colleges		$55	
FLSA Public Sector Compliance Guide		$95	

FREE EXPRESSION	QTY	COST	TOTAL
Free Expression on College Campuses		$75	
HARASSMENT/DISCRIMINATION/RETALIATION			
Preventing Harassment, Discrimination and Retaliation in the Academic Setting/Environment		$75	
INVESTIGATIONS			
Finding the Facts: Disciplinary and Harassment Investigations		$75	
LABOR RELATIONS			
Labor Relations: Collective Bargaining in Community College Districts		$75	
Labor Relations Fundamentals for CCDs		$75	
Unfair Practice Charges and PERB		$55	
LEAVES			
Leave Rights for California Community College Employees		$75	
PRIVACY			
Privacy Issues in the Community College Workplace		$75	
RETIREMENT			
Retirement Issues for California's Community Colleges & K-12 School Districts		$75	
SUPERVISION AND MANAGEMENT			
12 Steps to Avoiding Liability		$55	
Best Practices in Personnel Management		$75	
Prevention and Control of Absenteeism and Abuse of Leave in Community College Districts		$55	
VIOLENCE IN THE WORKPLACE			
Promoting Safety in Community College Districts		$75	

Name: _____

Title: _____

College/District: _____

Address: _____

_____

Phone: _____ Email: _____

To order these workbooks online and to view the Tables of Contents, please visit:
www.lcwlegal.com/news/workbooks

You can also submit your order by:

MAIL: 6033 W. Century Blvd., 5th Floor
Los Angeles, CA 90045

FAX: (310) 337-0837

Please make your check payable to:
LIEBERT CASSIDY WHITMORE

For further information, please contact the LCW Training Department at (310) 981-2000 or info@lcwlegal.com

Subtotal:	
CA Sales Tax: (for your city)	
Total Enclosed:	

LCW reserves the right to cancel any orders and/or refuse to process any orders, at its discretion.