I. What Is Invasion of Privacy?

A. Restatement (Second) of Torts, 652A, identifies four separate torts

1. Unreasonable intrusion upon the seclusion of another;
2. Appropriation of the other's name or likeness;
3. Unreasonable publicity given to the other's private life;
4. Publicity that unreasonably places the other in a false light before the public.

B. Colorado recognizes the tort of invasion of privacy

   [W]hen unreasonable action in pursuing a debtor is taken, which foreseably will probably result in extreme mental anguish, embarrassment, humiliation or mental suffering and injury to a person of ordinary sensibilities . . . then such conduct falls within the forbidden area and a claim for invasion of privacy may be asserted.

2. Employers should consider whether employees have a "reasonable expectation of privacy" in an area of an individual's life before they decide whether they may intrude upon or violate that area.

3. Wells v. Premier Indus. Corp., 691 P.2d 765 (Colo. App. 1984), a disclosure by employer to the IRS of employee tax information was not an invasion of privacy.

4. Colorado law also has specific statutory provisions for protection of privacy and personal freedom.

C. Constitutional rights to privacy

1. Federal courts have defined the federal constitutional right to privacy under the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments to the U.S. Constitution.


3. Constitutional right to privacy applies only to governmental actions. However, see discussion of public policy exception to at-will employment rule.

II. Investigating Employees and Applicants

A. Negligent hiring

1. Failing to investigate an applicant can give rise to claims for negligent hiring if the applicant is hired and subsequently injures another employee. Unfortunately, many employee "defects" are not readily discernable. Nevertheless, the courts are imposing a duty on employers to take reasonable precautions to prevent their employees from inflicting injury on others. If an employer knows (or has reason to know) of an applicant's dangerous propensities B perhaps because of a criminal record B and hires the person anyway, the employer will likely be found liable if the employee subsequently injures another person as a result of the employment. See, e.g., Gaines v. Monsanto Co., 655 S.W.2d 68 (Mo. App. 1983) (negligent hiring claim based on theory that employer knew or should have known that its mail clerk had previously been convicted of rape and robbery, that employer would have known he posed a danger to fellow employees if it had obtained such information, and that the mail clerk could not have killed the fellow employee if defendant had not hired him). Connes v. Molalla Trans. Sys., Inc., 831 P.2d 1316 (Colo. 1992).

2. Wise employers attempt to check all references on, and to conduct full background investigations on, applicants
they are about to hire, even when they believe no information will be uncovered or obtained. See Connes, 831 P.2d at 1321 ("Where the employment calls for minimum contact between the employee and other persons, there may be no reason for an employer to conduct any investigation of the applicant's background beyond obtaining past employment information and personal data during the initial interview. . . . We endorse the proposition that where an employer hires a person for a job requiring frequent contact with members of the public, or involving close contact with particular persons as a result of a special relationship between such persons and the employer, the employer's duty of reasonable care is not satisfied by a mere review of personal data disclosed by the applicant on a job application form or during a personal interview.")

B. Criminal records. Employers should consider investigating applicants' and employees' criminal records. However, the following also should be taken into consideration.

1. Colorado law prohibits forcing an employee to disclose criminal records which have been sealed. C.R.S. ' 24-72-308(3)(f)(I).

2. Making employment decisions based on arrest records (as opposed to convictions) arguably violates the public policy which presumes that all people are innocent until proven guilty.

3. Making employment decisions based on arrest records or criminal records can give rise to claims for disparate impact discrimination. However, an employer may, under certain circumstances, make decisions based on such records. When doing so, employers should make sure (i) that they are conviction records, and (ii) that the crimes committed can be linked to job-related qualifications.

C. Financial information

1. Tort actions. Colorado employers have faced invasion of privacy claims for wrongfully obtaining financial information about their employees. See Robyn v. Phillips Petroleum Co., 774 F. Supp. 587 (D. Colo. 1991). In Robyn, a former employee discovered that her personnel file included a copy of her bank statement. 774 F. Supp. at 591. The employee filed tort actions based on outrageous conduct and invasion of privacy. The court dismissed both claims because there was no indication of how the employer had obtained the information. Robyn, 774 F. Supp. at 591-92.

2. Fair Credit Reporting Act

a. Overview of the FCRA. Employers should be wary of the statutory restrictions on gathering information on applicants and employees, found in the Fair Credit Reporting Act ("FCRA"). The FCRA was passed in 1970 to regulate the credit reporting industry and assure that those involved in the business of obtaining and disseminating personal financial information adopt reasonable procedures to protect the accuracy and confidentiality of that information. The FCRA was amended as of October 1, 1997, in such a way as to provide significant protections for applicants and employees. Sanctions for violations may include criminal sanctions and civil penalties.

b. Impact on employers. Under the FCRA, a consumer report may be used to establish a person's eligibility for employment. The term "consumer report" applies to information gathered by a "consumer reporting agency" for an employer for "employment purposes," such as a criminal background check on an applicant, 16 C.F.R. Pt. 600, App. ' 603(d)(4)(D) (January 1, 1997); see also 15 U.S.C. ' 1681k(2). However, the employer must satisfy several conditions first. The employer must certify in writing to the consumer reporting agency that it will not use any report in violation of applicable employment discrimination laws or regulations. 15 U.S.C. ' 1681b(b)(1)(A)(ii). Second, the employer must certify in writing to the consumer reporting agency that it has "clearly and conspicuously" disclosed to the employee or applicant, in writing and in a separate document, that it may obtain a consumer report for employment purposes. Third, the employer must certify that the employee or applicant has authorized the procurement of the report by the employer. Fourth, the employer must make such disclosures and obtain the required written authorization. Fifth, the employer must certify in writing to the agency that, before it takes any adverse action regarding the applicant or employee, "based in whole or in part on the report," the employer will provide the person with a copy of the report and a writing describing the individual's rights under the FCRA. Sixth, the employer must follow through on these certifications, by providing the individual with a copy of the report before taking any
adverse action based on the report, as well as a written summary of employee rights under the FCRA.

c. Practical considerations

(1) If you need to obtain background information on an applicant or employee, you may avoid FCRA issues by not using a "credit reporting agency."

(2) If you must hire a credit reporting agency, obtain written consent from the individual in advance, using a consent form related only to the individual's rights under the FCRA and to the employer's obtaining information from a credit reporting agency. A consent in an employment application is not sufficient.

3. Discrimination claims. The EEOC "Guide to Pre-Employment Inquiries" advises that using credit history to screen applicants has been found to have a disparate impact on minorities and could therefore give rise to a disparate impact discrimination claim.

D. Polygraph tests

1. Under the Employee Polygraph Protection Act of 1988 ("EPPA"), polygraphs may not be used as applicant screening devices in most industries, and they are substantially restricted throughout private employment.

2. The EPPA covers only private employers. It exempts (i) companies that provide security services related to public health and safety, (ii) securities dealers, and (iii) pharmaceutical companies.

3. The EPPA effectively eliminates the use of polygraphs as pre-employment screening devices.

4. The EPPA bans use of polygraphs by private employers in employment situations except where the employer is investigating a specific incident and certain disclosures are given to the employee before the test is administered and certain procedural safeguards are followed.

5. An employer may not base an adverse employment action solely on the results of a polygraph.

6. Before a test can be administered the employee must be advised that she cannot be required to take the test as a condition of employment.

7. Violations of the EPPA can result in civil penalties of up to $10,000 and a party aggrieved by such an action has a cause of action for equitable relief and damages.

E. Employee searches

1. In general, private employers are not restricted by the confines of the Fourth Amendment which protects parties from unreasonable searches. See United States v. Jacobsen, 466 U.S. 109 (1984).

2. However, an unreasonable search could give rise to claims for damages based on the common law tort of invasion of privacy. See K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984) (search of an employee's locker was an invasion of privacy which gave rise to damages).

III. Personnel and Medical Information

A. Applicable laws

1. Americans With Disabilities Act ("ADA"). The ADA and Section 503 of the Rehabilitation Act impose restrictions on the collection, filing, and use of employee medical records.

   a. Collecting and filing of medical records
(1) Information regarding an applicant's or employee's medical condition and history must be collected and maintained on separate forms. 42 U.S.C. ' 12112(d)(3)(B).

(2) Such information must be stored in separate files. Id. Therefore an employer should not include any medical information in an employee's non-medical personnel file, even if that means redacting medical information from medical documents. See EEOC Preemployment Guide, & 140, 175.

(3) Confidentiality requirements continue to apply after the individual is no longer an employee or an applicant.

b. Access to medical records. All medical information must be kept confidential, except that the following people may have access to it or be informed of the applicant's or employee's medical condition:

(1) Supervisors and managers may be informed as to necessary restrictions on the work or duties of an employee and necessary accommodations. 42 U.S.C. ' 12112(d)(3)(B)(i).

(2) First aid and safety personnel may be informed if the disability might require emergency treatment. 42 U.S.C. ' 12112(d)(3)(B)(ii).

(3) Government officials investigating compliance with the ADA shall be provided with relevant information upon request. 42 U.S.C. ' 12112(d)(3)(B)(iii).

c. Use of medical information. The ADA restricts the use of employee and applicant information to purposes contemplated by Title I of the ADA. 42 U.S.C. ' 12112(d)(3)(C).

(1) An employer cannot require a medical examination or make inquiries regarding whether the person is an individual with a disability or as to the nature or severity of the disability, unless the examination is job-related and consistent with business necessity. 42 U.S.C. ' 12112(d)(4)(A).

(2) After an offer of employment has been made, an employer may require a medical examination or make inquiries "into the ability of an applicant to perform job-related functions." 42 U.S.C. ' 12112(d)(2)(B).

(3) An employer may conduct voluntary medical examinations, including voluntary medical histories, which are part of an employee health program available to employees at that work site. 42 U.S.C. ' 12112(d)(4)(B).

(4) Medical information may be used, to the extent necessary, to determine what reasonable accommodation should be made.

(5) Medical information may be used, to the extent necessary, to determine whether an individual poses "a direct threat to the health and safety of other individuals in the workplace." 42 U.S.C. ' 12113(b).

(6) An employer may use information that an individual has an infectious or communicable disease that is transmitted to others through the handling of food, which cannot be minimized through reasonable accommodations, to refuse to assign or continue to assign such an individual to a job involving food handling. 42 U.S.C. ' 12112(d)(2).

d. Illegal drug use

(1) The term "qualified individual with a disability" does not include applicants and employees currently engaging in the illegal use of drugs. 42 U.S.C. ' 12112(a).

(2) A test to determine the illegal use of drugs is not considered a "medical examination" within the meaning of Title I of the ADA. 42 U.S.C. ' 12112(d)(1).
The ADA expressly states that Congress, in passing that legislation, was not encouraging, prohibiting, or authorizing conducting drug testing for the illegal use of drugs or making employment decisions based on those test results. 42 U.S.C. \(12112(d)(2)\).

2. Colorado law. No Colorado statute specifically governs access to personnel records. However, regulations issued by the Colorado Civil Rights Commission restrict access to employee medical records.

   a. Collecting and filing of medical records. Like the ADA, the state regulations require the collection and maintenance on separate forms of any medical information relating to employees. 3 C.C.R. 708-1, Rule 60.2 (E)(4).

   b. Access to medical records. Like the ADA, the state regulations restrict access to medical records except for the circumstances under which the ADA provides for access.

   c. Use of medical information. Like the ADA, the Colorado regulations restrict the use of employee and applicant information.

      (1) An employer may condition an offer of employment on the results of a medical examination conducted prior to beginning work if all eligible employees are subject to such an examination regardless of disability and if the results of the examination are used solely to inquire into an applicant's ability to perform job-related functions. Id.

      (2) If an employer has taken remedial action to correct the effects of past discrimination or when an employer is taking affirmative action, the employer may invite applicants for employment to indicate whether and to what extent they are physically disabled provided that:

         (a) The employer states clearly on any written questionnaire used for this purpose, or makes clear orally, that the information requested is intended for use solely in connection with its remedial action obligations or its voluntary or affirmative action efforts; and

         (b) Employer states clearly that the information is being requested on a voluntary basis, that it will be kept confidential, that the refusal to provide it will not subject the applicant or employee to any adverse treatment, and that such information will be used only in accordance with remedial and affirmative action. Id.

B. Employee access

1. State law. Colorado has no statutory requirement that employers reveal employment files to employees. Therefore, employees have no right of access to their personnel files. Some state statutes entitle employees to review their own employment files. Therefore, multistate companies may wish to develop a broad policy that satisfies all jurisdictions without trying to manage the technicalities.

2. OSHA. This statute requires that employees be provided access to certain types of medical and accident information.

   a. Occupational Injury and Illness Log and Summary. Pursuant to 29 C.F.R \(1904.7\), the log and summary of all occupational injuries and illnesses required to be recorded under OSHA's requirements, must, upon request, be made available by an employer to any employee, former employee, or their representatives for examination and copying in a reasonable manner and at reasonable times.

   b. Employee exposure records. Except for certain trade secret protections, employers are required, upon request, to provide access to employees to any record relating to that employee concerning exposure to toxic substances. 29 C.F.R. \(1910.1020(e)(2)\).

   c. Employee medical records. Employees, upon request, are also entitled to access to employee medical records pertaining to the employee unless a physician representing the employer believes that direct access to
3. Investigations. In most instances, files relating to an investigation of an employee in response, e.g., to an allegation of sexual harassment, should be placed in separate files to which the employee is not permitted access. This policy should be followed regardless of whether the employee seeking access is the alleged victim or the alleged perpetrator.

   a. Attorney-client privilege and work product. Investigations, when conducted by or under the direction of counsel, can be subject to a claim of attorney work product or attorney client privilege protection. However, those protections could be waived by placing investigative materials in a file to which the employee or someone else, who was not involved in the investigative process, may have access.

   b. Privacy issues. Investigators, to the extent possible, should respect the privacy of the alleged victim, the alleged perpetrator, and any witnesses. Maintaining a separate file will help accomplish this objective.

   c. Retaliation. Although an employer may disclose some or all of the allegations to the alleged perpetrator to give him or her an opportunity to respond to the charges, the employer also may want to keep confidential certain inflammatory statements or details, especially if they are not directly relevant, to minimize the chance that the alleged perpetrator will attempt to retaliate against the alleged victim and any witnesses.

4. Other practical concerns. If possible, it makes sense to provide employees access to their own personnel files. Refusal to provide this access creates the impression that the employer is engaging in a cover up. Employers who do allow access to employee records should adopt a policy that clearly sets forth the means for gaining access. However, in the absence of clear and conspicuous disclaimers, such policies may be legally enforceable, as a matter of implied contract law. See Continental Air Lines, Inc. v. Keenan, 731 P.2d 708 (Colo. 1987).

5. Privacy Protection Study Commission. In 1977, this Federal commission issued guidelines for employers to use in handling personnel files. The recommendations are not legally binding, and have not been adopted by the Colorado legislature. The commission recommended that employers: (i) articulate, communicate, and implement fair information practice policies for employment records; (ii) inform employees of what records are maintained and how they will be used; (iii) adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of personnel records; (iv) permit individual employees to see, copy, correct, or amend their personnel records; (v) limit internal and external disclosure of personnel records; and (vi) monitor compliance with the company's fair information policy.

C. What may be released and when

1. ADA

   a. Additional permissible disclosures. In addition to the circumstances described in Section IV.A for requesting and using medical information, the ADA has been interpreted by the EEOC to allow disclosure in other circumstances.

      (1) Employers may submit information to State workers' compensation offices or second injury funds in accordance with State workers' compensation laws. 29 C.F.R. pt. 1630 app. ' 1630.14(b).

      (2) Employers who establish, sponsor, observe or administer benefit plans, such as health and life insurance plans, may use medical information for those purposes without running afoul of the ADA if the information is used for the development and administration of benefit plans. Id. at 1630.16(f).

   b. Inquiries by co-workers. In some circumstances, co-workers may inquire about either the physical or mental condition of a co-worker or a reasonable accommodation which is being provided to one worker but not others.

      (1) If a co-worker asks questions about another employee's disability, no medical information should be
disclosed, unless the person inquiring is covered by one of the exceptions discussed in Part IV.A.1.b, above.

(2) Similarly, an employer may not disclose that an employee is receiving a reasonable accommodation because this usually amounts to a disclosure that the individual has a disability. An employer may certainly respond to a question from an employee about why a co-worker is receiving what is perceived as "different" or "special" treatment by emphasizing its policy of assisting any employee who encounters difficulties in the workplace. The employer also may find it helpful to point out that many of the workplace issues encountered by employees are personal, and that, in these circumstances, it is the employer's policy to respect employee privacy. An employer may be able to make this point effectively by reassuring the employee asking the question that his or her privacy would similarly be respected if she or he found it necessary to ask the employer for some kind of workplace change for personal reasons.

Employers also might find it helpful, as a general matter, to provide all employees with information about various laws that require employers to meet certain employee needs, while also requiring them to protect the privacy of employees. In providing general ADA information to employees, an employer may wish to highlight the obligation to provide reasonable accommodation, including the interactive process and different types of reasonable accommodations, and the statutes' confidentiality protections.

Employers may wish to explore methods of providing this information to unions because they, too, are bound by the ADA's confidentiality provisions. Union meetings and bulletin boards may be further avenues for such educational efforts.

However, as long as there is no coercion by an employer, an employee with a disability may voluntarily choose to disclose to co-workers her or his disability and/or the fact that she or he is receiving a reasonable accommodation. See EEOC Enforcement Guidance: Reasonable Accommodation and Undue Hardship Under the Americans with Disabilities Act.

2. Tort claims for release of medical information. Employers must take care not to share employees' medical information when giving references about former employees. Such disclosure may violate the ADA. See e.g., Cossette v. Minnesota Power & Light, 188 F.3d 964 (8th Cir. 1999) (disclosure by former supervisor to prospective employer that employee had back injury and lifting restrictions constituted a violation of the ADA). Disclosing medical information could also constitute invasion of privacy if the disclosure is unauthorized and/or unnecessary. See Bratt v. International Bus. Mach. Corp., 467 N.E.2d 126 (Mass. 1984) (communication of medical information about an employee can be an invasion of privacy). Disclosing medical information also could support a claim for outrageous conduct/intentional infliction of emotional distress. See e.g., French v. U.S.A., 55 F. Supp. 2d 379 (W.D.N.C. 1999) (disclosure by former employer that employee had AIDS constituted extreme and outrageous conduct).

3. Colorado law. Colorado has no statutory provision which directly addresses the use of employee files. Generally, employees probably have a reasonable expectation of privacy in their employment files. Accordingly, dissemination of information outside a company could give rise to invasion of privacy and other tort claims. Therefore, the wisest course of action is to keep private information about employees confidential.

4. Practical concerns. Employment files should be treated as confidential documents and not shared within a company beyond those who have business reasons for the information. All of those individuals should be admonished to maintain the confidentiality of material in personnel files.

5. Sample personnel records policy. ABC Corp. has adopted the following basic policies regarding our employees' personnel records: (1) The Company will collect employee information only as needed for business or legal purposes; (2) The Company will maintain the confidentiality of all personal information in employee records, and will not release personal information to individuals outside the Company unless authorized by the employee or legally compelled to do so; (3) The Company will restrict access to authorized employees with a "need to know" or others only when legally compelled to do so; (4) Employees may review annually the information contained in their personnel files. Employees may submit a written statement responding to documents in their files. Staff who handle personnel records must adhere to these basic policies or face disciplinary action.
6. Releases. Before disclosing any current or former employee's records, consider requiring the requesting party to produce a written, notarized release signed by the employee authorizing the disclosure of records. The release should specifically state that all records should be disclosed or that only certain specific records should be disclosed. If in doubt, require clarification.

7. Responding to subpoenas. To ensure that they do not violate their employees' privacy rights, companies responding to subpoenas should consider the following actions: (i) have all subpoenas directed to one individual such as the human resources director; (ii) request more time to respond, if needed to consider the employee's privacy rights and consult with an attorney; (iii) consult with the employee whose records have been requested, and consult with legal counsel if the employee objects to production; (iv) produce only documents that are responsive to the subpoena that the company is compelled to produce; and (v) ask the attorney issuing the subpoena to modify any overly broad requests.

8. Employee Assistance Programs ("EAP"). EAP files should be treated as confidential records. The files from EAP programs may or may not be available to employers depending on whether the EAP is operated by a separate entity. Employers with an EAP should consider whether to notify employees that information revealed by them in the course of counseling or treatment may be disclosed to management, and to direct EAP service providers that information indicating an employee's dangerous propensities must be provided to management. Doe v. Garcia, 961 P.2d 1181, 1183 (Idaho 1998) (an employee's admission to the employer's EAP counselor that he had been fired from previous employment for sexually molesting a patient put employer on notice of his sexually dangerous propensities, supporting negligent supervision claim for employee's molestation of another minor).

D. Giving references for former and current employees

1. There is no requirement in Colorado for an employer to give a reference for current or former employee to a prospective employer.

2. If a reference is given, Colo. Rev. Stat. ' 8-2-114 provides a means for avoiding liability.

   a. C.R.S. ' 8-2-114 provides that an employer shall not maintain blacklist -- credit lists excepted -- immunity for good faith disclosures.

   b. It is unlawful for any employer to maintain a blacklist, or to notify any other employer that any current or former employee has been blacklisted by such employer, for the purpose of preventing such employee from receiving employment.

   c. Nothing in sections 8-2-112 to 8-2-115 prevents a former employer of any such employee from imparting a fair and unbiased opinion of such employee's qualifications when solicited so to do by a later or prospective employer of such employee. Sections 8-2-112 to 8-2-115 shall not be construed to prevent any merchant or professional person, or any association of the same, from maintaining or publishing a list concerning the credit or financial responsibility of any person dealing with them on credit.

   d. Any employer that, upon request by a prospective employer or a current or former employee, provides fair and unbiased information about a current or former employee's job performance, as provided in subsection (1) of this section, is presumed to be acting in good faith and shall be immune from civil liability for such disclosure and the consequences of such disclosure. For purposes of this paragraph (a) only, the presumption of good faith may be rebutted upon a showing by a preponderance of the evidence that the information disclosed was knowingly false, deliberately misleading, disclosed for a malicious purpose, or violative of a civil right of the employee, as protected under part 4 of article 34 of title 24, C.R.S.

   e. Any employer that provides written information to a prospective employer about a current or a former employee shall send a copy of the information provided to the last known address of the person who is the subject of the reference. Any person who is the subject of such a reference may obtain a copy of the reference information by appearing at the employer's or former employer's place of business during normal working hours. The employer or former employer may charge a fair and reasonable amount for reproduction costs if multiple copies are requested.
3. Avoiding liability

a. If a reference is not given, an impression is conveyed by the employer, which may or may not support a claim for liability.

b. If the employer has an absolute policy not to give references regarding any employee, and always follows that policy, then a statement of the policy may be used as a response to any individual request. This generally avoids any liability.

c. Employers can safely verify dates of employment and salary.

d. If an employer refuses to verify employment, this may be some indirect evidence of bad faith relating to one or more legal theories.

e. If an employer has a written policy about references, the policy should be followed. If references are discretionary for supervisors to give, both the accuracy of the references and any use of discretion must be monitored by the employer.

4. Other statutory protections

a. Colo. Rev. Stat. ' 8-2-111.5 -- Applying to banks, savings and loan institutions, and other lending institutions:

   (1) The financial institution may disclose information to a similar entity about any involvement in a dishonest act, such as theft, embezzlement, or misappropriation.

   (2) There is no civil liability if the statement is provided in good faith, which is presumed unless it is shown by a preponderance of the evidence that the institution, officer, director, or employee intentionally or recklessly disclosed false information about the employee or former employee.

b. Colo. Rev. Stat. ' 18-8-115 -- Sets forth the duty to report a crime to law enforcement. An employer may disclose information concerning a suspected crime "for the purpose of giving notice of the possibility that such other such criminal conduct may be attempted which may affect the persons or corporations notified. There is immunity from civil liability "when acting in good faith."

5. Claims that arise from employer references

a. Although claims generally do not arise from good or positive references, in Randi W. v. Muroc Joint Unified School District 12 IER Cases (BNA) 673 (Ca. 1/27/97), the California Supreme Court found that a student molested by a teacher could sue the teacher's former school districts for writing positive recommendations for him without mentioning that he had been involved in prior sexual misconduct.

b. Forms of retaliation. In Robinson v. Shell Oil Co., 519 U.S. 337, 117 S. Ct. 843, 136 L.Ed. 2d 808, 72 FEP Cases 1856 (1997), the United States Supreme Court held unanimously that an adverse employment reference could constitute retaliation against a former employee under Title VII's prohibition. In Robinson, an employee claimed retaliation against him for filing an EEOC charge and pursuing his civil rights.

c. Intentional interference with contract (employment relationship). If an individual violates company policy for individual malicious reasons, the claim against the individual may not be within the statutory immunity or the common law qualified privilege.

d. Defamation

   (1) In Churchey v. Adolph Coors Co., the Colorado Supreme Court states that "[a] cause of action for defamation requires, at a minimum, publication of a false statement of defamatory fact." 759 P.2d 1336, 1341 (Colo. 1988). "If the communication is protected by a >qualified privilege,' then the
plaintiff may recover only if he proves that the defendant published the material with malice, that is, knowing the matter to be false, or acted with reckless disregard as to its veracity." Thompson v. Public Service Co. of Colo. 800 P.2d 1299, 1306 (citing Churchey at 759 P.2d 1346).

(2) In Pittman v. Larson Distributing Co., 724 P.2d 1379 (Colo. App. 1986) the court noted that defamatory statements can be either per quod, i.e., requiring extrinsic facts to explain the defamatory character of the statement, or per se. In Pittman, the plaintiff sued his former employer for defamatory comments made by his prior supervisor to various third parties. The supervisor stated that the plaintiff was fired because "he wasn't doing as good of a job" and because he "spent too much time in the office on the telephone." The Colorado Court of Appeals held that these statements amounted to a per se defamation claim. The Court held that where an employer publishes a statement to a third party which is "defamatory of the plaintiff's trade, business or profession," a per se defamation claim is established. Id. at 1387 (emphasis added). The Court further explained that a per se claim does not require proof of damages they are presumed. Id.

(3) Qualified privilege. In Meehan v. Amax Oil & Gass, Inc., 796 F. Supp 461 (D.Colo. 1992) the court noted: "A qualified privilege extends to communications by a party with a legitimate interest to persons having a corresponding interest in communications promoting legitimate individual, group, or public interest . . . . However, the common interest privilege is only qualified or conditional. The privilege is lost if the statement is published with malice. A publication is malicious if the publisher knows the statement is false, or makes the statement with reckless disregard as to its truth or falsity."

IV. Employee Monitoring and Surveillance

Employers have many legitimate reasons for wanting to monitor employees' various forms of electronic communications, including, e-mails, voice mail, and Internet usage. Those reasons include preventing employees from wasting time while on the job, protecting trade secrets, and avoiding liability for discrimination or sexual harassment. No doubt, employees have certain rights to privacy in the workplace. However, whether any of those rights preclude an employer from monitoring employees' electronic communications has not yet been decided.

A. The dos and don'ts of telephone monitoring

1. Differences between business and personal telephone calls. The rules governing the monitoring of employee telephone calls vary depending upon whether the employer is monitoring business calls or personal calls. Generally, the random monitoring of employees' business telephone calls, pursuant to a policy announced to employers in advance, using ordinary telephone extensions, does not violate the wiretap law. James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979). On the other hand, an employer may not monitor employees' personal telephone calls, except for a brief period of time to determine whether the call is business or personal. The differences between monitoring business and personal telephone calls turns on the application of the federal wiretapping law.

2. The federal wiretapping law. The federal wiretapping statute, as amended by the Electronic Communications Privacy Act (ECPA), imposes civil liability on "any person who . . . (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept any wire, oral, or electronic communication" or "(b) intentionally endeavors to use, or procures any other person to use or endeavor to use any electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. ' 2510(4). Employers who violate the federal wiretapping statute can be subject to criminal prosecution and significant civil damages. 18 U.S.C. 2511(1), 2520. Despite the general prohibition on monitoring telephone calls, the ECPA provides two exceptions to the wiretapping law. These exceptions are the consent exception, and the ordinary course of business exception.

a. The consent exception to telephone monitoring. Under the consent exception, there is no liability for intercepting a telephone conversation when one party to the conversation consents to the interception. 18 U.S.C. ' 2511 (2)(d). This consent may be either express or implied. However, an employee who merely knows that calls are sometimes monitored has not consented to having every call monitored. Watkins v. L.M. Berry Co., 704 F.2d 577, 581-82 (11th Cir. 1983). Additionally, an employee has not consented to the monitoring of telephone calls just because he suspects that the calls are being monitored by the employer. Abbott v. Village of Winthrop Harbor, 1998 U.S. Dist. Lexis 11897 (N.D. Ill. July 23, 1998). On the other
hand, once the employer has expressly advised the employee that a telephone line is being monitored, any subsequent telephone conversations on that line are undertaken with consent to the monitoring. Id.

b. The ordinary course of business exception. Under this exception, anyone may listen to a telephone conversation from another extension, as long as the extension is an ordinary piece of equipment provided by the telephone service, and the interception is in the ordinary course of business. 18 U.S.C. ' 2510(5)(a)(i). This exception is applicable if the employer has a business justification for monitoring the call, and the recording is conducted around the clock in a non-discriminatory manner. See Arias v. Mutual Central Alarm Serv. Inc., 1998 U.S. Dist. Lexis 14414 (S.D.N.Y. Sept. 14, 1998). Additionally, when an employer suspects employee wrongdoing, and is investigating such, the employer may be permitted to listen in on and record employee telephone calls for a limited period of time. See Briggs v. American Air Filter Co., 630 F.2d 414, 420 (11th Cir. 1980). The employer, however, may only listen as long as necessary because this exception has been rejected when an employer listens and records an employee's telephone conversation longer than reasonably justified. See Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992). For example, in Deal, the court reasoned that the employer's suspicions of employee theft did not justify the recording of 22 hours of personal conversations.

3. The Colorado wiretapping statute. Colorado has a wiretapping statute similar to the federal statute. Colo. Rev. Stat. ' 18-9-301. In addition to ordinary telephone communications, the Colorado statute covers electronically stored communications and cordless telephones. Colo. Rev. Stat. ' 18-9-301 (3.3)(a), (3.7). Employers who violate the statute are subject to criminal prosecution. Colo. Rev. Stat. ' 18-9-303(2). The business purpose exception is valid only if the employer provides public notice that it monitors the telephone conversations. People v. McCauley, 561 P.2d 335 (Colo. 1977). In McCauley, the employer hired a private investigator to install recording devices on the telephones. The private investigator was convicted of wiretapping because as the employer's agent he failed to provide notice of the monitoring.

B. Computer monitoring

1. Changes in the federal wiretapping law. The original federal wiretapping law applied only to the interception of oral and wire communications carried by a common carrier -- in other words, face-to-face conversations and telephone calls over a public utility. 18 U.S.C. ' 2510(1), (2), (4). By the mid-80s, however, Congress noted a "dramatic change in new computer and telecommunications technologies." S. Rep. No. 99-541, 99th Cong., 2d Sess. reprinted in 1986 U.S.C.C.A.N. 3555, 3590. Because of the dramatic changes in technology, Congress enacted the ECPA to bring the existing wiretapping laws "in line with technological developments and changes in the structure of the telecommunications industry." Id.

a. The difference between the interception and retrieval of electronic communications. The ECPA provides two different, and inconsistent, standards governing when employers may obtain employees' electronic communications. The ECPA apparently grants employers almost unlimited access to employees' electronic communications when the employer simply retrieves an electronic communication from computer storage, as opposed to intercepting an electronic communication. An employer may intercept electronic communications only "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. ' 2511(2)(a)(I).

b. Example of when system providers may search computer files. An employer may examine computer files if the employer provides the computer system. Bohach v. City of Reno, 1996 WL 420439 (D. Nev. July 23, 1996). Because the federal wiretapping statutes distinguish between electronic communications and files electronically stored on a computer, providers of computer systems have full access to all files stored on the system. Compare 18 U.S.C. ' 2510(12) with 18 U.S.C. ' 2701 (c)(1)

2. Employers can probably monitor their employees' internet activities. Employers have a legitimate concern over their employees' Internet usage. An employee's productivity may be decreased because of the excessive time they spend on the Internet, and there is good reason for concern that the employees may download or display sexually harassing, profane, or other unprofessional materials on the employers' computer system. The courts have not clearly addressed the Internet in this context, but the cases on electronic communications and computer files should
protect employers who monitor their employees' activities. The monitoring of Internet sites visited by employees constitutes the interception of a wire communication, but the business extension exception of the ECPA allows such interception on standard equipment for a business purpose.

3. Policy regarding the monitoring of internet usage. A recent criminal case clearly indicates that it is prudent for an employer to implement a policy providing for the monitoring of employees' Internet use. In United States v. Simons, 1998 U.S. Dist. Lexis 19646 (E.D. Va. Dec. 15, 1998), a manager discovered that the defendant had downloaded thousands of pornographic pictures off of the Internet. The CIA had a written policy expressly providing for audits of the network "to support identification, termination, and prosecution of unauthorized activity." The policy also required supervisors to "ensure[ ] appropriate Internet use for all employees under their direction." Because of these policy statements, the Court ruled that the defendant had no reasonable expectation of privacy in his Internet access files.

C. Electronic communications: e-mail and voice mail. The permissible scope of monitoring e-mail and voice mail is not yet clear. In drafting the ECPA, however, it appears that Congress was concerned mainly with interception of electronic communications by strangers.

1. Employers can probably monitor e-mail. An employer's monitoring of e-mail is treated similarly to the monitoring of phone calls. Thus, the restrictions of the ECPA come into play. While the ECPA prohibits the interception of e-mail, three primary exceptions exist: a) the consent exception; b) the ordinary course of business exception; and c) as the provider of the electronic communications, the employer may monitor the lines to ensure adequate service. See U.S.C. ' 2511.

   a. Case law concerning e-mail monitoring. In Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Penn. 1996), an at-will employee was discharged for sending unprofessional communications on the company e-mail, despite the employer's prior assurance that e-mail communications would not be intercepted and that messages were private and confidential. The employee sued on the theory that his termination in these circumstances violated Pennsylvania's public policy against invasions of privacy. The Smyth court found that this public policy exception exists only for a "substantial and highly offensive invasion of the employee's privacy." Smyth, 914 F. Supp. at 100. In dismissing the employee's suit, the court applied tests derived from the Fourth Amendment to determine how substantial and offensive the invasion was. The court found that the company's interest in preventing unprofessional comments outweighed the employee's weak privacy interests in his e-mail. Smyth, 914 F. Supp. at 101.

   b. In Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996), a federal district court addressed privacy issues concerning an "alphage system," which is a program similar to e-mail, when two police officers sought to block an investigation of their messages. The alphage system allowed the police officers to send alphanumeric messages to a pager. The police chief barred messages that were critical of department policy, or were discriminatory in nature. The court reasoned that the officers did not establish a reasonable expectation of privacy, and that the search of computer stored messages was consistent with the federal wiretapping statutes.

2. Employers probably cannot monitor voice mail. Unlike e-mail, the courts have not yet addressed an employer's monitoring of employee voice mail. Generally, employers are barred from intercepting voice mail messages, which are treated throughout the ECPA as though they were ordinary telephone calls. Thus, employers who monitor voice mail messages without a legitimate business purpose should expect to be sued over such action. For example, the Wall Street Journal reported on a case where an employee sued his employer because his co-worker intercepted romantic messages left on the employee's voice mail. The co-worker played the messages for both the employer and the employee's wife. The employee claimed that he had a reasonable expectation of privacy based on the "secret access code" provided by the employer along with the assurances that the employee's voice mail was private. See Frances A. McMorris, "Is Office Voice Mail Private? Don't Bet On It," The Wall Street Journal B1 (Feb 28, 1995). Unfortunately, there is no reported decision on this case.

D. Other surveillance technology - knowing your legal boundaries. With the advent of modern technologies, many employers are resorting to video surveillance in the workplace. Again, employers need to be cognizant of their employees' privacy rights. The most common type of video surveillance is the closed-circuit camera, which is generally used to prevent theft and violence.
1. Unconcealed video cameras. Visible video surveillance is the method least likely to be found unlawful. One court found that an employer's visible video surveillance was lawful because it was in the employees' plain view, and the employees had been informed of the cameras. Vega-Rodriguez v. Puerto Rico Tele. Co., 110 F.3d 174 (1st Cir. 1997). The court reasoned that the employer could have hired humans to monitor the activity, but instead, chose to utilize unconcealed video cameras not equipped with microphones.

2. Hidden video cameras. The legality of using hidden cameras depends upon whether the employees have a reasonable expectation of privacy in the area in which they are being videotaped. For example, a California court found that there was no expectation of privacy in the "release office" of the county jail. Thus, it was legal to install a hidden video camera in the "release office" to monitor alleged theft of prisoner property. Sacramento Cty. Deputy Sheriff's Assoc. v. County of Sacramento, 51 Cal. App. 4th 1468 (Cal. App. 1996).

3. General guidelines when using surveillance. Employers should make sure that the use of surveillance equipment is related to legitimate business concerns, such as safety and security, and that the surveillance is not placed in an area where employees have a reasonable expectation of privacy. Finally, employees should be notified that they are under surveillance.

E. Issues to consider before adopting a policy. Although no single set of procedures will work for all employers, before adopting a policy, employers should consider the following:

1. How much use of the company's e-mail and voice mail systems will be allowed?

2. Does the company want to place any restrictions at all on employees' use of the electronic communications system for personal communications?

3. Does the company want to tell employees that their communications may be monitored at any time, without prior notice? While this practice provides employers protection from legal claims, it could foster an atmosphere of mistrust.

4. The policy should tell employees that messages are not private just because the employee has a password, and electronic messages that are deleted can be retrieved by the system administrator.

5. The policy should remind employees that e-mails sometimes become evidence in lawsuits and that they should send only messages that they and the company would not be embarrassed to have others read.

6. The policy should state in strong terms that the company's e-mail and voice mail systems are not to be used to transmit: (a) messages that are sexually graphic, contain sexual overtures or innuendos, or contain profanity; (b) messages that are demeaning to persons of any particular gender, race, religion, national origin, or sexual orientation; or (c) messages that have no business purpose and that would be unwelcome or offensive to the recipients.

7. Companies that adopt a policy regarding employees' use of electronic communications must be prepared to stick to the policy and enforce it with all employees.

F. Sample policies. In light of the uncertainty over how the courts will apply the ECPA and the common law of invasion of privacy to claims by employees arising from monitoring of electronic communications, employers should protect themselves by adopting policies and obtaining employee consent.

1. Electronic communication sample policy. Company XYZ provides e-mail and Internet services, as well as computer access and voice mail to its employees. Access to these services should be treated like any other means of communication and used appropriately. For example, as with Company XYZ's telephone system, you must minimize personal use. Similarly, you must regulate the types of communication you send and receive. Discriminatory or harassing communications, or communications of an obscene or sexual nature, are not permitted. If you abuse e-mail, Internet, computer, or voice mail services, you will lose your privileges with respect to such services and may be subject to discipline, up to and including termination. It is important for you to understand that our computer systems, including our e-mail, Internet, and voice mail systems belong to Company XYZ. We expect
that these systems will be used for business purposes. We therefore reserve the right to retrieve, store, and inspect communications that you compose, send, receive, or store on these systems. There should be no expectation of privacy for electronic communications. You may be asked, as a condition of your employment at Company XYZ, to sign an acknowledgment form concerning this policy.

2. Employee acknowledgment sample form. I understand that all electronic communication systems and all information transmitted by, received from, or stored in these systems are the property of XYZ Company. I also understand that all electronic communication systems are to be used solely for job-related purposes, and that I have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt, or storage of information in this equipment. I agree not to access a file, or retrieve any stored communication unless authorized. I acknowledge and consent to Company XYZ monitoring my use of this equipment at any time at its discretion. Such monitoring may include printing and/or reading all e-mail entering, leaving, or stored in Company XYZ's system as well as listening to my voice mail messages in the ordinary course of business.

V. Sexual Harassment Investigations

A. General guidelines

1. Take action.

2. Take every complaint seriously.

3. Act promptly.

4. In order to avoid any inference that an employer is implicitly endorsing or tolerating sexual harassment, employers should act on complaints promptly.

5. A prompt response will stop harassment and build employee confidence in the process.

6. Even if you reach the conclusion that sexual harassment has not occurred, a prompt investigation builds employer credibility and demonstrates that harassment will not be tolerated.

B. Determine whether harassment has occurred

1. General investigation guidelines

   a. Get the facts: who, what, when, where.

   b. Do not be judgmental.

   c. Limit access to results of investigation.

   d. Advise witnesses to keep the investigation confidential.

   e. If possible, do not disclose information with questions. Ask general questions such as "Describe Jane's interactions with John," rather than "Did you see John grab Jane?"

   f. Interview the victim, the alleged harasser and potential witnesses.

2. Interviewing the alleged victim

3. Get specifics

   a. Basic facts

      (1) Pattern v. single incident.
(2) Others involved.
(3) Physical v. verbal harassment.
(4) Sexual v. non-sexual abuse.
(5) Obtain dates, times and frequency of conduct.

b. Determine the context: work, after hours, joking, serious.

c. Determine whether the conduct was "unwelcome"

   (1) Did the victim participate in activities?
   (2) Did victim give a clear message "No"?
   (3) Why might victim have legitimately failed to send a clear "No"?
   (4) Past relationship between the parties.

d. Determine the effect on the alleged victim

   (1) Economic losses.
   (2) Psychological injury.
   (3) Physical injury.
   (4) Threats to job security.

e. How long since the incident occurred is the alleged victim reporting?

f. Find out if there are any witnesses or documents.

g. Examine the alleged victim's motives. For example, has she just been criticized for poor performance?

h. Determine what the alleged victim wants

   (1) Fire the harasser;
   (2) Warn the harasser;
   (3) Job security;
   (4) Reassignment; and/or
   (5) Counselling.

i. Assure the alleged victim that she will not be retaliated against for making the complaint.

j. Make no statements about the accused's character.

4. Interview alleged harasser

   a. Ask the accused about the charges
(1) Be specific.

(2) Expect denials.

b. Ask for explanations from the alleged harasser

c. Determine the accused's relationship with the alleged victim

   (1) Does he have any power over her? E.g., supervisor-subordinate.

   (2) If appropriate, determine whether they have an intimate relationship or a past intimate relationship.

d. Inquire as to whether the accused has any motive to allege sexual harassment.

e. Determine whether there were any witnesses to the alleged harassment.

5. Interview witnesses

   a. Question witnesses to the alleged harassment.

   b. Assure witnesses that their testimony will be kept confidential and that they will not be retaliated against for testifying.

   c. Do not defame the accused with the questions you ask.

6. Interview other potential victims

   a. Identify other subordinates and/or coworkers and determine whether they have been subjected to conduct similar to that alleged.

   b. If the EEOC investigates, it will consider the existence or absence of such other conduct.

7. Look for evidence of past similar conduct

   a. Are there any previous complaints about sexual harassment?

   b. Examine personnel files and consider interviewing supervisors for evidence of other similar conduct.

C. Recordkeeping

1. Keep records of all complaints.

2. Make records of the investigation.

3. Do not put the records in the employee's or the alleged harasser's personnel files.

4. Consulting your lawyer, even briefly, before the investigation will help create a confidentiality privilege for the results.

D. Take corrective action

1. Failure to take corrective action could make the employer liable for the conduct.

2. Taking overly severe corrective action could lead to liability to the accused.
VI. Miscellaneous Employee Privacy Issues

A. Social relationships

1. It is unlawful to discriminate against someone based on the fact that they are married to another employee.

   a. C.R.S. '24-34-402 (1)(h) provides:
   It shall be a discriminatory or unfair employment practice . . . (I) For any employer to discharge any
   employee or refuse to hire a person solely on the basis that such employee or person is married to or plans to
   marry another employee of the employer.

   b. The statute does not apply to employers with less than 25 employees.

   c. The statute does not apply where:

      (1) "One spouse directly or indirectly would exercise supervisory, appointment, or dismissal authority
      or disciplinary action over the other spouse," or

      (2) "One spouse would audit, verify, receive, or be entrusted with moneys received or handled by the
      other spouse," or

      (3) "One spouse has access to the employer's confidential information, including payroll and personnel
      records."

2. Lawful off-duty activities

   a. Personal relationships are also, in most situations, lawful, off-duty activities, protected by C.R.S. '24-34-
   402.5.

   b. If those activities significantly impact on the workplace, however, they would not be protected.

   c. Employers must be careful to draw the link between off-duty relationships and objective, verifiable impacts
   on the workplace if they wish to take actions based on those relationships.

3. Sexual harassment

   a. One type of sexual harassment, so-called quid pro quo harassment, involves the perception or the reality
   that in order to get ahead an employee must engage in a personal relationship with the boss.

   b. Accordingly, one significant area of concern related to personal relationships in the workplace is that
   favoritism towards a paramour or spouse could gives rise to claims for quid pro quo sexual harassment.

   c. Employers must balance these concerns against the need to respect employee privacy and the need not to
   take action based on lawful, off-duty activities.

   d. The best solution is probably not to allow people involved in a relationship or people who are married to be
   in supervisor-subordinate roles in the workplace.

4. Relationship policies

   a. Strict policy against fraternization

      (1) Difficult to enforce
(2) Potentially violate privacy rights.

(3) Force relationships underground

b. Policy permitting non-supervisor/subordinate relationships

(1) Require notice to company when relationship develops so that steps can be taken to avoid actual or perceived favoritism and retribution.

(2) Requiring notice allows a company to manage the situation, while recognizing the reality that relationships will exist in the work place. It also give the company a defense if an employee who did not give notice later complains.

c. Elements of a policy

(1) Identify prohibited conduct

(2) Establish guidelines for off-duty activities

(3) Define permitted and prohibited relationships

(4) Establish enforcement guidelines

(a) If a work place relationship develops, and the company transfers the subordinate employee to avoid the issues described above, then this could be seen as retaliation against the subordinate. If the subordinate is also a woman, then it looks like gender discrimination, i.e., penalize the woman when they both had the affair.

(b) Establishing guidelines ahead of time, before there are any particular individuals involved, gives the company a solid argument against discrimination.

(5) Train employees.

B. Associations

1. Associating with others is lawful, off duty activity which is most likely protected.

2. Certain associations enjoy additional express protection

   a. C.R.S. ' 8-2-102 provides: "It is unlawful for any . . . company . . . to prevent employees from forming, joining, or belonging to any lawful labor organization, union, society, or political party."

   b. C.R.S. ' 8-2-103 provides a penalty for violating the above provision of up to $500 and one year in jail.

   c. C.R.S. ' 8-2-108 states that employers may not prohibit their employees from engaging in political activities or running for political office.

C. Dress and grooming codes

1. Dress and grooming codes are generally enforceable and legally permissible. That is, you can require employees to wear their hair in certain ways and dress in certain ways as a precondition of being employed. There are, however, several significant exceptions.

2. Exceptions

   a. Religious discrimination
(1) Companies must affirmatively accommodate religious beliefs and practices.

b. Gender discrimination

(1) Women permitted to wear ponytails and earrings, but not men.

(2) This distinction is enforceable so long as the employees are working with the public and the company has a bona fide business interest in presenting a certain image.

c. Disparate impact claims

(1) Some rules, neutral on their face, can have a disparate impact on minority groups.

(2) For example, a rule against beards can have a disparate impact on African Americans more prone to certain skin irritation and conditions resulting from shaving.

D. Conduct codes

1. Generally, an employer is free to impose terms and conditions on employee behavior during work hours.

2. Rules in union (or concerted activity) situations

   a. Speech either for or against union activity is protected in the work place. Employers must allow union speech to the same extent that they allow other groups to speak in the work place. Thus, for example, an employer that permits political organizations to advocate for their causes, e.g., save the whales, must also permit union speech to the same extent.

   b. Employers that have collective bargaining agreements cannot impose new terms or conditions of employment without first bargaining to an impasse.

3. Codes of conduct directed at off duty activity are limited by the rule prohibiting discrimination based on lawful off-duty activity discussed above.

   a. In Gwin v. Chesrown Chevrolet, Inc., 931 P.2d 466 (Colo.App. 1996), the Colorado Court of Appeals held that the prohibition of the statute applies regardless of whether the employer has adopted a rule that attempts to restrict off-duty activities of its employees.

   b. In Marsh v. Delta Air Lines, Inc., 952 F. Supp. 1458 (D.Colo. 1997), the court held that activities of an employee that breach the implied bona fide occupational requirement of loyalty provided a basis for the employers utilization of the exceptions to the general prohibition of the statute. In Marsh, the employer was justified in terminating an employee who had written a letter critical of certain business decisions made by the employer. In dicta, the court indicated that if the letter had addressed matters of public concern, as opposed to merely private business decisions of the employer, the result might have been different. 952 F. Supp. at 1463.