WORKPLACE PRIVACY IN THE DIGITAL AGE

I. VARIOUS ISSUES OF PRIVACY IN THE WORKPLACE

A. Employment Applications and Interviewing – The types of information that can be collected from a prospective employee in an application for employment, or during an interview prior to an offer of employment.

B. Applicant Screening:

1. Fingerprinting

2. Background Checks (Criminal History, Driving Records, Educational Records, Licensures)

3. Reference Checks

C. Employee Personnel Files and Personal Information Maintained by the Employer

D. The Disclosure of Employee Personal Information to Third Parties

E. Physical Searches of Employees and Their Workplaces

F. Drug Testing of Employees or Candidates

G. Electronic Monitoring

1. Equipment Provided by Employer versus Employee (e.g. Cell Phone, Computer)

2. Emails and Internet Use by Employees

3. Telephone, Voicemail or Fax Use by Employees

4. Video and Audio Surveillance of Employees

H. Social Media

1. Employer Surveillance of Employee Social Media Use

2. On or Off of the Clock

3. Adverse Action Based on Actions or Statements Made by Employee on Social Media Site

I. Constitutional Issues: Public Employers and an Employee's Right to Privacy and Unreasonable Searches and Seizures

II. APPLICANT SCREENING – BACKGROUND CHECKS

A. Background Checks

1. Before deciding whether to use a background check, employers should assess the particular credentials and requirements an employee should possess and the tasks the employee may engage in for each job position offered and whether a background check would assist the employer in assessing a candidate's qualifications for that particular job position.

a) There should be a legitimate and rational business reason why the employer is requesting a background check.

2. Before making any employment decision, including the hiring of a prospective employee based on the applicant's criminal history, an employer should consider the following factors:

a) The gravity and nature of the offense or conduct;

b) The length of time since the offense, conduct, or conviction and the completion of any sentence;

c) The nature of the job sought;

d) The relationship between the job sought and the record of conviction;

e) The number of convictions;

f) Rehabilitation efforts; and

g) Subsequent employment history.

3. Note that there are various State and Federal laws that regulate the use of conviction and arrest records in the context of employment decisions.

4. Employers should always obtain prior written authorization from the prospective employee prior to performing background checks.

B. Fair Credit Reporting Act

1. The Act regulates persons or entities which obtain and/or use consumer reports and in which circumstances the contents of those reports may be used.

2. Credit Reporting Agencies provide background credit, financial, and other personal information on consumers (including prospective or current employees) – payment history, addresses, criminal histories, driving records, etc.

3. The employer may only obtain a consumer report for a permissible purpose, such as an employer's evaluation of an individual for employment, promotion, reassignment or retention.

4. The Act requires that prior to obtaining a consumer report an employer must:

a) Make a clear disclaimer to the employee or prospective employee in writing that a consumer report may be obtained for employment purposes; and

b) The employee or prospective employee must provide written consent to the employer to run a consumer report.

5. Prior to taking any adverse action against an individual, the employer must provide the employee or prospective employee with a copy of the consumer report, and a written statement of the individual's rights

under the law (the FTC has published a form for users of consumer reports to hand out).

6. If an adverse decision is made based in whole or in part on information contained in the consumer report, the employer must provide orally, in writing, or electronically to the employee or prospective employee:

   a) Notice of the adverse action;

   b) The name, address, and telephone number of the credit reporting agency that provided the consumer report;

   c) A statement that the credit reporting agency did not make the negative decision and cannot provide the individual with the particular reasons supporting the adverse action; and

   d) Notice of the person's right to obtain a free copy of the consumer report (if requested to the agency within 60 days upon receipt of notice from the employer); and

   e) Notice of the person's right to dispute the accuracy and completeness of the information contained in the consumer report.

7. Investigative Consumer Reports – Special rules apply. Investigative Consumer Reports include personal information obtained through personal interviews with people associated in the community with the consumer about whom the report is being created.

   a) Prior to obtaining an investigative consumer report the employer must disclose in writing (mailed or otherwise delivered) within three days after the report was first requested that such a report was requested, such writing which includes a statement informing the person of his or her rights to request a summary of the nature and scope of the investigation conducted and a written summary of his or her rights; and

b) If the employee / prospective employee requests a summary of the nature and scope of the investigation the employer must mail that summary to the employee / prospective employee within five days of its receipt of the request or within five days the report is first requested, whichever comes later.

8. The FCRA and other Federal and State Laws prescribe what types of information may be included or must be excluded from consumer reports.

a) Criminal Arrests and Convictions. Under the FCRA reports of arrests can only go back 7 years; conviction records can go back indefinitely. State laws may prohibit the reporting of arrests or convictions all together or beyond a certain prescribed time. For example, under Michigan law an employer cannot, in connection with an application for employment or in connection with the terms, conditions or privileges of employment, request a record of information regarding misdemeanor arrests that did not result in conviction.

b) Driving Records. Under the Driver's Privacy Protection Act of 1994, State departments of motor vehicles can only release personal information of motor vehicle operators under limited circumstances (i.e. to verify personal information in connection with a valid driver's license). Personal information includes identifying information such as a name, address and social security number, but does not include information on vehicular accidents, driving violations and driver's status.

III. ELECTRONIC MONITORING

A. Electronic monitoring includes the monitoring of an employee's emails, internet, fax and telephone use, and video and audio surveillance.

B. Purposes of Monitoring are to ensure that employees are using business products and equipment properly (i.e. for business purposes), to deter theft and violence, and to limit employer liability.

C. Public Employers should keep in mind constitutional rights of Employees prior to instituting any policies pertaining to surveillance and searching.

D. An Employee's Expectation of Privacy:

1. Employees have a lesser expectation of privacy in public and common areas.

2. Employees have greater expectations of privacy in bathrooms and locker rooms.

3. An employer can lower an employee's expectation of privacy by providing all of its employees with clear explanations of the employer's electronic monitoring policies and procedures both at the time of hire and on a routine basis (with a signed acknowledgment from the employee).

E. Electronic Communications Privacy Act

1. The ECPA makes it illegal for anyone to intentionally intercept or cause another person to intercept or endeavor to intercept wire, oral, or electronic communications. The Act also makes it illegal in certain circumstances to access stored wire or electronic communications without authorization.

2. Phone conversations.

a) An employer may monitor phone conversations if one of the party's to the conversation consents (e.g. the employee), or if the employer is the owner of the equipment (employer) and the interception occurs in the ordinary course of business. There must be a legitimate business purpose for monitoring without consent and in such case monitoring must be routine.

b) If the conversations are personal in nature the employer must immediately stop monitoring.

c) In the case of telemarketers and customer service monitoring, a recorded message should be played for all callers and

employees should all be notified that their conversations are being recorded.

3. Michigan Eavesdropping Statute. This law makes it a crime to use any device to eavesdrop upon a private conversation without the consent of all the parties to the conversation whether present or not in the conversation. Eavesdropping includes to overhear, record, amplify or transmit any part of the private discourse without the consent of all persons engaged. Civil damages may also be obtained under this statute.

4. Email Use.

   a) Courts have not resolved the issue of whether intercepting emails while in transit from sender to recipient violates the ECPA.

   b) Employers may search stored emails if the employer maintains the system on which the message is stored.

   c) Internet Use

   d) Employers can monitor internet usage on computer systems maintained or provided for by the employer.

IV. SOCIAL MEDIA

A. Issues with Social Media Use:

1. An employer accessing information about a current or prospective employee that is related to protected characteristics of said employee (e.g. age, sex, religion, disability, marital status, etc.) – just the fact that the employer had access to said information may create the inference of an improper motive for taking adverse action against the current or prospective employee.

2. Accessing Social Media Sites during work hours either on employer equipment or employee's personal equipment causing lower productivity.

3. Posting about work-related issues on-duty and/or off-duty.

4. Posting confidential information of the employer.

5. Need of employer to ensure productivity of employees and address issues for which the employer may be liable (e.g. liability for unaddressed discrimination, harassment, or defamation).

B. Michigan Internet Privacy Protection Act.

1. The Act prohibits employers from requesting an employee or an applicant to grant access to or to view that employee's or applicant's personal internet accounts, or to take adverse action against the employee or applicant for refusing to provide such access.

2. The Act does not prohibit an employer from accessing information stored or transmitted through devices provided for or paid for in whole or in part by the employer, so long as such accessing is done in compliance with other state and federal laws (e.g. Electronic Communications Privacy Act)

3. The act does not prohibit the employer from accessing an account or service provided by the Employer to the Employee for use within the employee's employment and/or the employer's business.

4. The Act does not prohibit the employer from disciplining an employee for transferring the employer's proprietary or confidential information without employer authorization.

5. The Act does not prohibit the employer from conducting an investigation if there exists specific information about activity on the employee's personal internet account for the purpose of ensuring compliance with the law or prohibitions against work-related misconduct or information about unauthorized transfers of proprietary or confidential information related to the employer.

6. The Act does not prohibit an employer from restricting access to certain websites on employer-provided equipment.

C. Employers:

1. Should avoid obtaining access to social media/networking sites by using false pretenses or placing the employee under duress.

2. Publically available information okay to access.

3. Should refrain from using information pertaining to protected characteristics in its employment decisions.

D. Discipline. If an employee's conduct violates an employer's social media policy and does not fall within the National Labor Relation Act's protections (or other applicable state laws), an employer usually may discipline the employee.

1. See below for a discussion on appropriate ways for an employer to structure a social media policy.

V. MANAGING PRIVACY IN THE WORKPLACE

A. Goals of Managing Privacy in the Workplace:

1. Key goal of employer to maintain a safe and productive work environment.

2. Key goal of employer to ensure company products and equipment are used appropriately by employees.

3. Avoiding unnecessary litigation or other disputes.

4. Balancing an employer's need to monitor with an employee's rights and expectation of privacy.

5. Managing the employee's expectations of privacy while maintaining employee morale.

6. Providing a company-wide framework and guidelines for managers / supervisors to deal with various employee-related Issues.

B. Written Privacy and Social Media Policies; Employee Handbooks

1. Key is to focus on an employee's reasonable expectation of privacy – Make the policy reasonable.

2. An employer must carefully draft the policy so as not to violate the employee's rights.

3. The policy should be communicated to all employees on a routine basis. Therefore, copies of the policies should be included in the orientation process for employment (i.e. Hiring Paperwork).

4. The employer should require the employee to sign an acknowledgement that he or she received and reviewed the policy and understands its contents.

5. The policy should outline all procedures that may be used to monitor or search.

6. The employer should equally and consistently apply and enforce the policy.

7. The employer should review the policy routinely to ensure changes in the employer's needs or the law can be addressed by the policy; the updated policy should then be communicated to all employees.

8. The employer should post all of its written policies in areas frequented by employees.

9. Social Media Policies.

    a) They should be reasonable.

    b) Social media policy should be very particular as to the types of information an employee cannot post about (e.g. trade secrets and confidential information of the employer).

    c) The policies should be very narrowly tailored as to not infringe or appear to infringe on employee's rights, especially with respect to employees' rights to self-organize and engage in other concerted activities for the purpose of collective

bargaining or mutual aid and protection (Section 7 of the National Labor Relations Act) and other state and federal laws pertaining to social media (e.g. Michigan's Internet Privacy Protection Act).

(1) Note that as indicated in certain decisions by the National Labor Relations Board, a general savings clause contained in a social media policy or in an employee handbook is not always be enough to save broad, sweeping prohibitions in a social media policy.