

## What Every U.S. Employer Should Know About Workplace Privacy

*Part One of a Two-Part Series*

**By Lisa J. Sotto and Elisabeth M. McCarthy**

The U.S. privacy arena is a minefield for employers. The United States has no omnibus employee privacy law. Instead, employers are faced with a patchwork of privacy laws that they must piece together to avoid legal liability. This article focuses on the key privacy issues employers in the U.S. must confront.

### **BACKGROUND SCREENING**

According to a January 2004 survey by the Society for Human Resource Management, 82% of employers investigate the backgrounds of potential employees. Employers conduct background checks on job applicants not only to verify the candidates' credentials, but also to ensure workplace safety and avoid potentially devastating financial and reputational harms associated with negligent hiring, retention, and supervision claims. It is significantly less costly to conduct a thorough background check on a job applicant than to hire an employee with a history of violence, sexual harassment, or embezzlement. Conducting appropriate background checks has reached a new imperative since 9/11. This has been further fueled by the corporate scandals of 2002 involving companies such as Enron and WorldCom.

Employers typically ask consumer reporting agencies to assemble and evaluate information about a job applicant's professional and personal life. Certain jobs, such as those in the banking, childcare, health care, airline, and trucking industries require criminal background checks.

Many sources of information used in background checks are public records, including criminal, civil court, bankruptcy, tax lien, professional licensing, workers' compensation, and driving records. The Fair Credit Reporting Act ("FCRA") imposes restrictions on the inclusion of certain public records in background screening reports. For example, for positions with an annual salary of less than \$75,000, civil judgments and paid tax liens cannot be reported in a background screening report after 7 years, and bankruptcy filings cannot be reported after 10 years. In addition, records relating to an individual's arrest cannot be included in a background check report after 7 years. A criminal conviction, however, may be reported indefinitely. To the extent that an employer conducts a background check internally, these limitations do not apply. In the event a consumer reporting agency errs and includes in a report provided to the employer information beyond the applicable time limit, an employer would not be precluded from considering such information.

A job applicant or employee background check may also include an employment report from one or all three of the credit reporting agencies (Equifax, Experian, and TransUnion). An employment report contains information regarding an individual's credit payment history and other credit habits, but does not include the individual's credit score or date of birth. Employers often look at an individual's credit history as an indication of financial responsibility.

In addition, employers may seek to obtain education records relating to job applicants or current employees.

This type of information may include dates of attendance at educational institutions and degrees earned. Employers seeking information from education records, however, may be restricted in gaining access to certain records without authorization from an adult-age student or parent due to restrictions set forth in the Family Educational Rights and Privacy Act.

Employers can also learn much about job applicants and employees by using an Internet search engine like Google. Employers likely will be able to determine information such as an individual's age, marital status, house value (complete with an aerial photograph), political affiliation, liens, blog entries, and more.

### ***Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act of 2003***

The FCRA was enacted in 1972 (and amended in 1996) to promote the accuracy, fairness, and privacy of personal information assembled by consumer reporting agencies. The FCRA allows consumer reporting agencies to furnish an entity with consumer reports only where the recipient has a permissible purpose to use the reports. Permissible purposes include use for employment purposes or use in connection with credit or insurance transactions. The FCRA defines a "consumer report" as "any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, which is used or collected in whole or in part for the purpose of serving as a factor in establishing the

*continued on page 2*

---

## Workplace Privacy

*continued from page 1*

consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; employment purposes; or any other permissible purpose authorized under 1681b."

The FCRA does not require that employers conduct background checks, but establishes national standards that employers must follow when screening potential employees or investigating current employees using consumer reports obtained from consumer reporting agencies.

Under the FCRA, an employer must disclose to the job applicant or employee that the employer will be retaining a consumer reporting agency to prepare a consumer report on the individual. This disclosure must be on a stand-alone document and not part of an employment application. The employer must receive the individual's signed consent to the preparation of such a report prior to requesting the report from the consumer reporting agency.

If the employer uses information contained in the consumer report for an "adverse action," such as failure to hire or promote, rescinding an existing job offer, or reassigning or demoting an existing employee, where such actions are based, in whole or in part, on information contained in the report, the employer must notify the subject of the report prior to taking the adverse action. This pre-adverse action notice must include a copy of the report and an explanation of the individual's rights under the FCRA. After the adverse action occurs, the employer must provide the individual

with an "adverse action notice." This notice would include the name, address, and phone number of the consumer reporting agency that prepared the report and statements that 1) the employer, and not the agency, made the adverse decision regarding the individual, 2) the individual has the right to a free copy of the report, and 3) the individual has the right to dispute the accuracy or completeness of the information contained in the consumer report.

The FCRA permits an employer to obtain a consumer report that has information about an individual's "character, general reputation, personal characteristics and mode of living" collected as a result of interviews with neighbors, friends, relatives, associates or others as part of an employment background check. Such reports are "investigative consumer reports." When an employer requests an "investigative consumer report," the FCRA requires that the employer provide written notice to the individual that the background report will include interviews, provide the individual with a statement of the nature and scope of the requested report and the individual's right to request additional details and, if requested, provide a written notice informing the subject of the report how to obtain a copy of his or her file. The employer must certify to the consumer reporting agency that the employer has provided the proper notice to the individual.

The FCRA also requires employers to certify to the consumer reporting agency that the employer 1) is requesting the report for a legitimate purpose (*ie*, investigation of a job applicant or existing employee), 2) has provided the employee or job applicant or employee with the requisite notice of the background check, 3) has obtained written permission from the employee or job applicant to request the background report, 4) will provide the applicant or employee with a copy of the report and written notice of the applicant's or employee's rights prior to taking an adverse action based in whole or in part on information contained in the background report, and

5) will use the background report only for employment purposes. The FCRA's notice and consent requirements do not apply to employers that conduct background checks internally rather than retaining a third-party consumer reporting agency to do so.

Employers that fail to comply with the FCRA's requirements may be liable to the individual that is the subject of the consumer report for actual damages, litigation costs, attorneys' fees, and punitive damages. Employers also may face criminal penalties for obtaining a credit report under false pretenses. The FCRA authorizes the Federal Trade Commission ("FTC") to enforce its provisions. The FTC may sue employers for up to \$2500 per violation of the FCRA.

A number of states have laws that contain provisions similar to the federal FCRA. Several states, including California and New York, have FCRA analogues that regulate the use of background screening for "employment purposes." Most state analogues provide protections similar to those found in the FCRA. To the extent an employer conducts background investigations in which it requests credit reports, it should 1) determine whether the relevant state has an FCRA analogue, and 2) if it does, comply with its requirements.

In 2003, the Fair and Accurate Credit Transactions Act ("FACTA") amended the FCRA to establish standards for "employee misconduct investigations." An "employee misconduct investigation" is an investigation of an employee which is conducted by a third party that the employer hires if the employer suspects the employee of workplace misconduct or noncompliance with federal, state, or local laws or regulations, pre-existing written policies of the employer, or rules of a self-regulatory organization. FACTA exempts from the definition of "consumer report" communications made by a third party to an employer in connection with an employee misconduct investigation. Consequently, an employer is not required to obtain an employee's consent before hiring a third party to investigate employee misconduct. If the employer decides

*continued on page 3*

---

**Lisa J. Sotto** is a partner in the New York office of Hunton & Williams LLP and heads the firm's Privacy and Information Management Practice. She also serves as Acting Chair of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. **Elisabeth M. McCarthy** is counsel in the New York office of Hunton & Williams LLP and advises clients on privacy and information management issues.

---

## **Workplace Privacy**

*continued from page 2*

to take an adverse action against an employee following an employee misconduct investigation, however, the employer must give the employee an “adverse action” notice after such adverse action has occurred.

The employer must provide the employee subject to the adverse action with a summary of the investigation report that resulted in the adverse action. The employer is not required to disclose the sources of information for the report or the identity of any witnesses. The investigation report must be kept confidential and may only be disclosed to the employer or the employer’s agent, governmental authorities, and the self-regulatory organization with regulatory authority over the employer or employee. FACTA does not permit an employee who is subject to an adverse action as a result of an investigation to dispute the findings contained in the report.

### **DISPOSING OF EMPLOYEE**

#### **PERSONAL INFORMATION**

##### ***FTC Rule on the Disposal of Consumer Report Information***

In November 2004, the FTC issued regulations requiring businesses to properly dispose of consumer report information. The rule, which became effective on June 1, 2005, was designed to help combat identity theft resulting from the improper disposal of information. The Disposal Rule requires companies to take reasonable steps to guard against unauthorized access to or use of consumer report information in connection with its disposal. It applies to any business that maintains or otherwise possesses “consumer information,” which is defined as “any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report ... [or] a compilation of such records.” Because employers frequently rely on consumer reports in connection with employment decisions, the Disposal Rule affects them. Information that does not identify individuals, such as aggregate or blind data, is not covered by the rule.

The Disposal Rule requires covered entities to properly dispose of consumer report information “by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.” “Disposal” includes:

- discarding or abandoning consumer information; and
- selling, donating, or transferring any medium, including computer equipment, on which consumer information is stored.

The rule does not define what is “reasonable,” instead allowing for a flexible standard that permits covered entities to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time. The rule includes specific examples of measures the FTC believes satisfy the rule’s disposal standard. These examples, which are intended as guidance and not as safe harbors or exclusive methods for compliance, include:

- implementing policies and procedures that require 1) the burning, pulverizing or shredding of papers containing consumer information, and 2) the destruction or erasure of electronic media containing consumer information, so the information cannot practicably be read or reconstructed;
- after conducting due diligence of the disposal company (which due diligence could include conducting an independent audit of the company’s operations, obtaining references, or requiring that the disposal company be certified), entering into a contract with the disposal company to dispose of consumer information in a manner consistent with the disposal rule;
- for disposal companies, implementing policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with the first example set forth above; and
- for entities subject to the Gramm-Leach-Bliley Act’s Safeguards Rule, incorporating the proper disposal of consumer information as

required by the disposal rule into the information security program required by the Safeguards Rule.

### **State Records Disposition Laws**

Several states also have laws that address the disposition of records containing personal information. Employers should determine whether the state in which they conduct business has enacted such a law and, if so, be sure to comply with its requirements.

### **SOCIAL SECURITY NUMBER LAWS**

Social Security Numbers (“SSNs”) were initially issued by the federal government for the purpose of administering Social Security programs. Over time, however, many businesses have taken to using SSNs as unique identifiers for individuals. As a result, SSNs have become a widely used device for managing employee files, medical records, health insurance records, credit and bank accounts, and educational records. In addition, SSNs are frequently printed on licenses and identification cards.

Limiting the widespread use of SSNs has become a major focus of state legislators seeking to curb identity theft. In an attempt to limit access to SSNs by unauthorized individuals, many states have enacted laws that limit their use or require that SSNs be redacted. At the end of 2005, at least 25 states had enacted laws restricting the use of SSNs.

At least 13 states prohibit printing an individual’s SSN on any card required for the individual to receive products or services provided by the person or entity issuing the card. Eight states prohibit printing SSNs on materials that are mailed to individuals unless otherwise required by federal or state law. A couple of states have chosen to allow redacted SSNs to be used in certain circumstances. A recent law enacted in California requires employers, by Jan. 1, 2008, to use no more than four digits of an employee’s SSN on checks or vouchers. As of Jan. 1, 2006, health insurance carriers in Washington state are prohibited from displaying on identification cards more than any four-digit portion of the subject person’s SSN. Delaware prohibits health insurers from using SSNs

*continued on page 4*

---

## ***Workplace Privacy***

*continued from page 3*

entirely as identification numbers on health insurance cards.

To date this year, at least 38 states have introduced additional legislation

restricting the use of SSNs. More states likely will follow with similar legislation. Employers should understand how their organization uses its employee SSNs and remain vigilant about the impact of evolving legal requirements.

*Next month's installment will discuss the Health Insurance Portability and Accountability Act of 1996, information security; and monitoring employee telephone, e-mail, and Internet use.*



---

**HUNTON &  
WILLIAMS**

Hunton & Williams LLP • [www.hunton.com](http://www.hunton.com)

Atlanta • Bangkok • Beijing • Brussels • Charlotte • Dallas • Houston • Knoxville • London • McLean • Miami • New York • Norfolk • Raleigh • Richmond • Singapore • Washington