BNA, INC.

WHITE COLLAR CRIME REPORT

BNA Employee-Owned Since 1947

JUNE 5, 2009

INTERNAL INVESTIGATIONS

Privacy Issues: Workplace Searches, Surveillance, and Monitoring

STEVEN P. SOLOW AND MEGHAN A. O'DONNELL

The Old Days, Old Ways Are Gone

Businesses know well that undetected employee misconduct creates a range of risks. Employees steal money, goods, and proprietary information, and they do so for their own gain or to assist competitors. Employee misconduct in the course of their employment can violate a wide range of workplace laws designed to protect other employees from harassment and discrimination and to protect worker safety and the environment. Employee misconduct can lead to violations of the growing thicket of federal laws related to corporate governance and financial disclosure, from the Sarbanes-Oxley Act and the Foreign Corrupt Practices Act to tax, accounting, and trading rules. Moreover, heavily regulated businesses in areas such as energy and futures trading face a level of scrutiny over their employees' conduct that can be measured in the time it takes to send a text message. Information security breaches are occurring ever more frequently and are a growing source of business risk and liability with new state and federal laws as well as international laws (particularly in the European Union) that raise significant issues for multinational employers. In the United States, whether or not the business knew or approved of such conduct, it can cause the business itself to be held civilly liable (for both regulatory violations and in tort) as well as criminally.

Steven P. Solow is a partner in the Washington, D.C., office of Katten Muchin Rosenman LLP, where he serves as Chair of the firm's Environmental Litigation Practice. He is a former chief of the Department of Justice Environmental Crimes Section and a co-author of the ABA's recent book "Environmental Litigation: Law & Strategy."

Not so long ago, a business could undertake an investigation of the employee(s) suspected of misconduct in these areas with relatively few restrictions. Moreover, the business had little concern that simply conducting the investigation could cause the business itself to incur liability. Those days are gone.

New Expectations. Today, businesses face a rising tide of expectations to prevent, detect, and effectively investigate and remedy the misconduct described above (as well as the many others you thought about while reading this far). Now they also need to do so in a manner

 ISSN 1559-3185

that does not run afoul of employee privacy protections. The expectations to act promptly come from many sources: state and local governments, shareholders, investors, employees, and the public at large (in the form of community groups, nongovernmental organizations, and tort plaintiffs, and the increasingly powerful ability of electronic media to send a message around the world before a memo can travel one floor up to land on your desk).[1]

The growing privacy and records management laws impose new liabilities related to the *manner and means* by which internal investigations are conducted. These requirements mirror many of the constitutional limitations that governmental entities face in conducting investigations: The investigation must be conducted in a manner that does not violate an ever-widening range of protections for employee privacy. This is why many businesses turn to those experienced in conducting or responding to government investigations for assistance.

For ease of analysis, we can divide the topic issue into two stages: setting limits and managing expectations *before* a problem arises, and properly managing the potential land mines when an issue arises and time is often of the essence.

Setting Limits and Managing Expectations

The time to address workplace privacy issues is not during an investigation. Unfortunately, that is often the time when a question may first arise such as, ''Can we look at this employee's private e-mail account?'' What follows is a very brief discussion of items that should be addressed by a company as early as today. Really.

I. Understand Your Universe of ESI

One of your first steps in undertaking any internal investigation requires the evaluation, with little substantive information and under much time pressure, of the nature of the documents and information (most likely electronically stored information, or ESI) that could be relevant to the investigation. The company should have a plan in place to allow coordination with those tasked with the investigation, records managers, and information technology personnel not only to understand the type of information stored and communications used by employees, but also to map out the location where that information resides. For example, employee e-mail—is it Lotus, Microsoft Exchange, or something else? Where do backup copies reside? How do you access e-mail in the active system? Many of these questions require the assistance of data consultants and/or outside counsel.

Methods of Communication. Your employees do not communicate solely via e-mail. Instant messaging, SMS texting via cell phones, or PIN-to-PIN texting via Blackberries or other messaging-enabled portable devices all provide the luxury of instantaneous communication and the burden of lax or nonexistent retention ability and a greater employee perspective of privacy on the content. Ownership of these devices greatly affects whether the employer can access communications transmitted via them.

Repositories of Documents and Data. If electronically stored written documents would be relevant, the company must find out what type of document management system it possesses. Are there shared network spaces that contain this information?

Databases and other types of structured data systems—financial enterprise resource planning systems, human resources, and IT databases—can also be repositories of relevant information. You need to work with IT to map the systems, understand how data can be exported, and know what information can be put on suspension, from routine system cleanup, overwriting, or deletion.

Does the company have off-site archival or disaster recovery backup media? This media, too, can be relevant. The company must gain an understanding of rotation schedules so that unintended destruction does not lead to claims of spoliation or obstruction.

II. Define Privacy Law That Would Be Implicated

Today, along with all the other challenges of an investigation, businesses must consider employee privacy issues before the investigation begins. In the United States, employers face few restrictions in connection with monitoring their employees' *activities* in the workplace. With respect to monitoring employee *e-mail*, however, at the federal level, the Electronic Communications Privacy Act governs the privacy protections related to electronic communications. ECPA prohibits the intentional interception of electronic communications, including e-mail, in transit. It does not, however, apply to communications in storage, such as an e-mail retained in an employee's inbox.[2] This broad general prohibition applies to ''any person,'' including private companies. Remedies for violations of ECPA include criminal and civil liability (violators are subject to imprisonment for up to five years and/or a fine of up to

[1] At a recent production of Ibsen's ''An Enemy of the People'' (in which the mayor, newspaper editor, and others in a small town stymie the efforts of a local doctor to disclose pollution from a local business), a young theatergoer could not buy into this basic premise of the story. The play, written toward the end of the 19th century, requires acceptance of the idea that the doctor could be prevented from getting his message to the public. The idea that someone could not get his message out (by e-mail, blogging, texting, or twittering) was too great a hurdle, and it made the premise so flawed as to make the tension of the play ''annoying.'' Communication is changing, including communication about corporate activities, at a pace that continues to outstrip the prior generation's comprehension.

[2] Some recent decisions, however, may indicate a contrary trend. When a current or former employee uses the company's Internet to communicate with an attorney, that communication may be privileged from disclosure. Recent caselaw suggests that use of the employer's computer system does not serve as the third-party presence to eliminate the privilege if the employee reasonably expected the communication to remain confidential. See Christopher Caparelli, *Employee E-Mail and the Attorney-Client Privilege*, LAW.COM, Nov. 7, 2007, at http://www.law.com/jsp/llf/PubArticleLLF.jsp?id=1194343439816. If the company maintains and enforces a policy banning personal use of the e-mail system, actively monitors the use of employee computers and e-mail, has access to the specific computer or e-mail account used, and notifies employees (or the employee is otherwise aware) of the active monitoring of these policies, then courts may find that the balance favors the company and deem that the privilege was waived. If, however, these factors are absent, then the investigators may be denied access to the information communicated to an outside attorney.

  WCR ISSN 1559-3185

$250,000 for individuals and $500,000 for organizations), and a private cause of action, including the greater of ''actual damages suffered by the plaintiff and any profits made by the violator,'' or statutory damages ($100 for each day of violation or $10,000), whichever is greater.

Lack of adequate and regular enforcement of a communications and use policy negates the notice provided by the policy because it creates ''a false sense of security which lull[s] employees into believing'' that the usage policy will not be enforced, thus rendering an employee's expectation of privacy in his or her communications reasonable.

The Stored Communications Act. The Stored Communications Act prohibits unauthorized access to a wire or electronic communication ''in electronic storage.'' ''Electronic storage'' is defined as, in part, ''any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.'' However, to the extent the company, as the user of the service, would be the one accessing the stored communications, the SCA might not be violated. The question turns, then, on whether the communication belongs to the company or to the employee. If the employee's communications are personal, or are sent from a personal account, the SCA may be implicated because the employee, rather than the company, could be considered the ''user of the service.''

Below the federal level, a few states have laws restricting an employer's right to monitor employee e-mail. Moreover, some states impose specific restrictions. Connecticut and Delaware, for example, require that before electronic monitoring can take place, the employer must inform its employees that the employer may conduct such monitoring.

Invasion of Privacy. In the United States, employees who believe their privacy rights have been violated by the employer viewing of employee communication may bring a claim against their employer using the common law tort of invasion of privacy. One element of this tort, the claim of ''intrusion upon seclusion,'' is the most common basis for workplace privacy actions.[3] To successfully assert such a claim, the employee must show that there was a reasonable expectation of privacy and that the employer invaded the employee's privacy. The success of these claims depends on whether a court believes the employee had a reasonable expectation of privacy, considering factors such as these: Was there a communications and use policy referencing the privacy of employee communications? Was the communication through a personal or a company account? Did the company adequately and consistently monitor and enforce its policy?

Outside the United States, workplace privacy regulation takes a markedly different form. For example, laws in the European Union strictly control workplace monitoring. As a result, a complex legal analysis, with assistance of local counsel from that country, is necessary before an employer may investigate employee behavior in the European Union. There is an additional layer of complexity as the permissibility of employee monitoring differs in each member state according to the strictures of local employment law. Additionally, if a company chooses later to export European-based information, it may encounter blocking statutes that bring with them potential fines and imprisonment.

III. Create, Distribute, Uniformly Enforce Policy

Grant Company Access, Disabuse Employees' Expectation of Privacy. Caselaw regarding whether an employee's communication was private considers and reflects the following principles:

- Employees generally have no reasonable expectation of privacy in the addresses of Web sites visited using employer-owned computers and the employer's Internet access.
- Employees might have a reasonable expectation of privacy in e-mails sent through private accounts, but that expectation may be ''nullified by explicit employer policies on computer use and monitoring.''[4]
- In order for the policy to be effective in nullifying any expectation of privacy or privilege, the employer must provide employees with an appropriately specific notice of its monitoring practices and properly enforce the policy.

If the employer's electronic communications policy (1) prohibits the use of employer systems for personal purposes, (2) specifies that employees have no right of personal privacy in any matter stored in, created, or sent over e-mail, voice mail, or employer Internet systems, and (3) provides notice that the employer has the right to monitor all data that flows through its systems, then the employee's expectation of privacy is not reasonable, even if the communication is sent through a password-protected personal account. In that situation, the company would not likely be held liable for a common law tort of invasion of privacy. Lack of adequate and regular enforcement of a communications and use policy, however, negates the notice provided by the policy because it creates ''a false sense of security which lull[s] employees into believing'' that the usage policy will not be enforced, thus rendering employees' expectation of privacy in their communications reasonable.[5]

[3] For a more thorough discussion of workplace privacy, see Lisa J. Sotto and Elisabeth McCarthy, *What Every U.S. Employer Should Know About Workplace Privacy*, PRIVACY & DATA PROTECTION LEGAL REPORTER, May & June 2006 (two-part series).

[4] *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863, *75 (D. Or. Sept. 15, 2004) (34 EMP. BENEFITS CAS. (BNA) 2097).

[5] *Curto v. Medical World Communications Inc.*, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. May 15, 2006); see also *Quon v. Arch Wireless Operation Co.,* 529 F.3d 892, 2008 WL 2440559 (9th Cir. June 18, 2008).

It is almost guaranteed that the call to conduct the investigation will come to you at approximately 4:48 p.m. (local time) on a Friday afternoon. Usually in June.

This means that businesses, before an investigation issue arises, should draft a carefully constructed communications use policy that prohibits using the employer's systems for personal communications or purposes, states that employees do not have a right of privacy in any matter stored, created, or sent through that system, even if through a personal account, and notifies the employees that the employer will monitor communications. Consider including this policy in the HR manual that each employee receives, request an acknowledgement signature, and regularly redistribute the policy as a reminder. Then, enforce the policy and document your efforts. Indications that the employees are disregarding the policy or do not believe it will be enforced requires prompt action to preserve your rights under the policy.

Unionized Employees. Do you wish to search the communications of unionized employees? Generally, privacy issues are proper subjects for bargaining, and a union employee's state law claim for invasion of privacy will be preempted by a collective bargaining agreement if the agreement contains provisions relevant to the claims.

Conducting the Internal Investigation In Light of Privacy Laws and Concerns

It is almost guaranteed that the call to conduct the investigation will come to you at approximately 4:48 p.m. (local time) on a Friday afternoon. Usually in June. The call will be from any of a number of people. It may be an internal call giving you a little more time to gather your forces and deploy them, or it may come from an outside number (the Securities and Exchange Commission, the Environmental Protection Agency, or Anderson Cooper). In any event, whether or not you have taken the steps and addressed the issues outlined above, you still have to act promptly. This is why the lawyers in our firm know that a call at approximately 4:58 p.m. that day is either a call from home (''When are you coming?'') or a call from a client (''When are you coming?'').

What follows are some of the key considerations for conducting the internal investigation in light of the range of privacy laws and concerns noted above.

Critical Steps in First Phase of Investigation

■ Seek to determine the nature of the allegations, the source of the information, and the potential that the allegations raise civil or criminal liability or may expose the company to other collateral consequences.

■ Evaluate the universe of people who may be reasonably considered to possess relevant documents and information. If appropriate, as soon as practicable, draft a legal hold tailored to the matter, distribute it to all relevant custodians, and request acknowledgment of receipt of the hold. Effective implementation of the hold will most likely require assistance from the IT department and/or consultants to complete such tasks as suspending auto-delete functions, expanding in-boxes, mapping servers to which the custodians' e-mail is stored, freezing or taking snapshots of mailboxes and shared spaces, etc., to assist in the prevention of any data loss.

■ Commence a status check of the company's policy for communication use. Is it up-to-date? Is it compliant with applicable privacy regulations? Has it been promulgated to all employees? Has it been regularly enforced? A company will expose itself to much risk if it proceeds in a manner that is inconsistent with its policies and manuals.

■ Identify the systems or employees covered by the investigation and develop a plan to gather available documents and other information to develop your factual story. Are there any other documented reports of related activity? This may entail interviews of employees to understand where particular employees related to the issue store their documents. Before interviewing, however, consult company policy and any union or arbitration agreements for possible restrictions or specific procedures in ''bringing employees in for questioning,'' and consider the best way to deploy both in-house and outside counsel.

■ Be careful that any review of personnel files of the employee(s) who may be the subject of the investigation are handled with appropriate confidentiality.

■ Determine how best to conduct interviews, including choosing individuals to conduct the interviews who are as separate as can be reasonably accommodated from the matter at issue. If lawyers are conducting the interviews, provide an appropriate *Upjohn* warning regarding the attorney-client privilege.

In the United States, whether or not the business knew or approved of such conduct, it can cause the business itself to be held civilly liable (for both regulatory violations and in tort), as well as criminally.

Gather e-mail and other electronic information in compliance with your pre-developed and distributed policy. Before gathering personal account e-mails saved on the company system, it is best to have some basis to believe that the information in the employee's personal account is needed information and that the company's policy makes such actions defensible. (Be cognizant of the potential for state laws to be more prescriptive in this area.)

These issues and steps are the beginning of the process that can critically affect the course of a matter if

   ISSN 1559-3185

they are handled properly in the first 24 hours and the first weeks of an investigation.[6]

[6] For further information on related topics, please see the following articles.

Lisa J. Sotto, John W. Woods Jr., and John J. Delionado, *Data Breach! Correct Response Crucial*, New York Law Journal (May 29, 2007).

Paula J. Bruening, Lisa J. Sotto, Martin E. Abrams, and Fred H. Cate, *Strategic Information Management*, Privacy & Sec. L. Rep. (BNA) (7 PVLR 1361, 9/15/08).

See also supra note 3.