WILLCOX & SAVAGE

EMPLOYMENT LAW OUTLOOK

21ST CENTURY TECHNOLOGY MEETS THE FLSA

Samuel J. Webster

Our society depends upon cell phones, smart phone technology, and portable laptop computers. Many of us carry smart phones that allow access to a host of data, and we find ourselves constantly checking and responding to e-mails when out of the office, even on vacation or in the middle of conversations. Laptop computers accompany us wherever we go for use at every opportunity. Text messaging proliferates. This explosion of timeless communication should cause employers concern for Fair Labor Standards Act compliance.

Congress enacted the Fair Labor Standards Act ("FLSA") at a time when the definition of "work" was fairly static: a person went to work at a certain hour and left at a certain hour and nothing on either side constituted "work." The FLSA establishes standards for the length of "work" and for paying overtime; generally, an employer must pay overtime for work exceeding 40 hours per week to employees who are not exempt from the FLSA's overtime requirements, usually "hourly employees." Exempt employees, salaried white collar management or professional employees, do not fall under FLSA's overtime rubric and their use of technology to expand the work day does not lead to additional compensation. However, for non-exempt employees, companies must be very careful whether or how they have those employees using any smart phone or other computer technology outside of normal working hours.

The Department of Labor ("DOL") has regulations covering "on-call" time. DOL distinguishes between "engaged to wait" and "waiting to be engaged." "Engaged to wait" means that the on-call person's ability to do personal tasks while on-call is severely, if not totally, limited. That time is compensable. At the other extreme, a person "waiting to be engaged" has little or no restriction on personal activities, local travel and response time. That time is not compensable except when actually engaged. In between the two lie the employees with cell phones, Blackberries®, other smart phone technology, and laptops, all of whom will challenge the employer's FLSA compliance efforts. For example, in August, the *Wall Street Journal* reported on several technology-related FLSA lawsuits: T-Mobile employees seeking overtime compensation for using company-issued smart phones to respond to work-related

(CONTINUED ON PAGE 3)

NLRB - IS RIP VAN WINKLE AWAKENING?

Thomas M. Lucas

Employee Free Choice Act ("EFCA") debate continues to rage, with several recent developments. In April 2009, Pennsylvania Senator Arlen Specter changed his party alliance, aligning himself with Democrats. Then, on September 22, he spoke at the AFL-CIO Convention and affirmed his support for the passage of EFCA. He predicted that before the end of 2009, Congress will pass EFCA-based labor legislation which will be "totally satisfactory to Labor." In his comments, Senator Specter detailed the revised EFCA bill:

- Maintain secret-ballot elections;
- "Quick" secret-ballot elections, as early as 21 days after filing of a petition;
- Guaranteed "equal access" for union organizers to employees on company time and property if employers hold "captive audience" meetings with employees;
- Stiffer penalties for unfair labor practices, both for companies and unions;
- "Last-best-offer arbitration" to establish terms of an initial collective bargaining agreement.

Senator Specter reportedly predicted that such a revised EFCA "package" will secure the 60 votes necessary to defeat a filibuster. Earlier, on September 11, Senator Harkin (D-Iowa), one of the lead Senate EFCA negotiators, revealed that in July, the Senate had worked out a "pretty good agreement" on a compromise EFCA package. President Obama has stated that "Change is finally having a President…who will make the Employee Free Choice Act the law of the land."

Regardless of whether EFCA passes in any form, what should not to be overlooked is that with an administration change comes changes of presidential appointees to the five-member National Labor Relations Board ("NLRB"). The NLRB has the power to significantly change case law and election procedures, essentially implementing "labor law reform," with or without the passage of EFCA. The Obama Administration appointments and nominations suggest that the new Board, once confirmed, may undertake substantial "labor law reform."

(CONTINUED ON PAGE 4)

HIPAA PRIVACY - NEW BREACH NOTIFICATION REQUIREMENTS

Luba I. Seliavski and Ruby W. Lee

HIPAA (Health Insurance Portability and Accountability Act of 1996) requires employers to maintain the privacy of employee health care information. In August, the Department of Health and Human Services ("HHS"), pursuant to the American Recovery and Reinvestment Act of 2009 ("ARRA"), published an interim final rule regarding the employer's duty to notify employees of breaches of HIPAA's privacy and security requirements. HHS requires employers to notify their employees of privacy breaches discovered on or after **September 23, 2009**.

Breach

A "breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the existing HIPAA privacy regulations, which then compromises the security or privacy of such information. However, the rule specifically excludes certain disclosures of **unsecured** protected health information from the definition of "breach." The rule triggers the breach notification requirement only if the breach of the unsecured protected health information poses a significant risk of financial, reputational, or other harm to the individual. While conducting a risk assessment, a HIPAA-covered entity and business associate should consider the following:

- Who impermissibly used the information or to whom was the information impermissibly disclosed;
- The type of information involved;
- Whether the covered entity took immediate steps that eliminated or reduced the risk of harm; and
- Whether the information was returned prior to being used for an improper purpose.

Unsecured Protected Health Information

ARRA defines "unsecured protected health information" as protected health information that is not secured through the use of technology or methodology specified by the Secretary. On April 17, 2009, the HHS Secretary issued a Guidance, which specifies that encryption of electronic protected health information and destruction of paper protected health information are the only two methods that make protected health information secure.

Discovery of Breach

A HIPAA-covered entity or business associate must notify its employees when it discovers a breach of unsecured protected health information. A breach is "discovered" when the covered entity or its agent has actual knowledge of the breach, or would have had actual knowledge had it exercised reasonable diligence.

Notice to Individuals

Once a breach is discovered, the employer must notify each individual whose unsecured protected health information has been breached without unreasonable delay, and no later than 60 days after discovery of the breach (subject to limited exceptions). The notice must be written in plain language and include the following: (i) a brief description of what happened, including the date of the breach and the date of its discovery; (ii) a description of the types of information involved; (iii) steps that the affected individuals should take to protect themselves; (iv) a brief description of the covered entity's investigation of the breach and what remedial steps it is taking; and (v) contact procedures for individuals to obtain more information.

Notice to Media

For a breach of unsecured protected health information that involves more than 500 residents of a state or jurisdiction, an employer must also notify "prominent media outlets" serving the jurisdiction or state without unreasonable delay, and no later than 60 days after discovery of the breach. Depending on where the affected individuals reside, appropriate media outlet may include a local newspaper or major general newspaper with a daily circulation throughout the state. The media notice does not substitute for individual notices.

Notice to Secretary

For breaches involving 500 or more individuals, an employer also must provide notice to the HHS Secretary in the manner indicated on the HHS Web site at the same time that it provides notice to the affected individuals. For breaches involving fewer than 500 individuals, the employer must document the breaches and notify the Secretary of all breaches occurring during that calendar year no later than 60 days after the end of the calendar year.

Notice by Business Associate

An employer's business associate (e.g. benefit plan administrator) must notify the employer of a breach of unsecured protected health information without unreasonable delay, no later than 60 days after discovering the breach. Notification to the employer must include the identification of each affected individual and any other available information that the employer must provide in its notice to the employee. As the discovery of the breach by a business associate starts the 60-day notification period to the affected individuals of the breach, a business associate should notify the employer as soon as the breach is discovered by the business associate.

Assuring HIPAA Compliance

Employers should take the following steps to assure compliance:

- Identify protected health information within the organization;
- Decide whether and how it will secure all protected health information as specified in the Secretary's Guidance;
- Develop policies and procedures for breach notifications, including guidelines for determining whether a breach that requires notification has occurred; and

(CONTINUED ON PAGE 3)

21ST CENTURY TECHNOLOGY MEETS THE FLSA

(CONTINUED FROM PAGE 1)

messages after hours; a CBRE maintenance worker suing for pay for time spent receiving and responding to messages on his cell phone after hours; Lincare employees seeking compensation for answering customer questions by cell phone while on-call.

DOL regulations governing compensation for "waiting" or "on-call" time require case specific factual determinations. The regulations provide a number of examples for on-duty waiting, off-duty waiting, and on-call time. The regulations' overriding theme is the extent to which the on-call employee's ability to engage in personal activities is affected. Employers must consider the following factors:

- Does the company place a geographic or response-time limitation upon the "on-call" employee?
- How frequently must the "on-call" employee actually be required to respond to calls?
- Is the "on-call" employee permitted to use a pager or cell phone, giving the employee more flexibility than sitting at home by the phone?
- What consequences exist for not responding to a call? Stated alternatively, how large is the pool of "on-call" responders?
- What agreement exists between the "on-call" employee and the company?

Generally, if (1) the required response time is reasonable (however long that is?), (2) the restrictions on travel are reasonable, (3) calls are not so frequent as to disrupt or eliminate personal activities, and (4) on-call time trading among employees is flexible, then the courts hold the time is not compensable. At the other end of the spectrum, if (1) the employee is required to stay on or very near the company's premises or travel is restricted, (2) the response time is relatively short (10-15 minutes), (3) the "on-call" time is lengthy (24/7 or variation), and (4) many calls occur during the waiting period, then the court is more likely to find the time compensable. Analysis of the travel time involved in responding to calls falls under the same guidelines.

Employers also face FLSA issues in actually accounting for the "on-call" time for non-exempt employees using the technology. The courts have fashioned a *di minimis* rule when the on-call work only involves a few minutes beyond the regularly scheduled hours. This rule turns on three factors:

- The administrative difficulty of recording the additional time;
- The aggregate amount of time spent; several *di minimis* calls or entries in one work day could add up to compensable time;
- Whether the employee regularly performed this type of work.

No court has set a minimum amount of time below which the work will be *di minimis*. Rather, courts conduct a fact-specific inquiry. The challenge, then, is tracking the time in order to get it into payroll.

Employers must continue to classify their employees carefully, erring toward non-exempt. Then, employers must take care regarding the extent to which they require their non-exempt hourly employees to carry and use cell phones, smart phone technology, and laptop computers. They also need to monitor that use carefully. Finally, they should train managers/supervisors on the potential pitfalls of relying upon the current technology without paying the non-exempt employees. Given the case-by-case factual analysis upon which these conflicts may turn, employers must take care with the interface of modern technology and their non-exempt employees. ■

HIPAA PRIVACY - NEW BREACH NOTIFICATION REQUIREMENTS

(CONTINUED FROM PAGE 2)

- Identify workforce members responsible for drafting and approving breach notices.

The HIPAA Privacy Rule also requires employers to do the following:

- Train members of its workforce on the policies and procedures with respect to breach notification;
- Provide a process for individuals to make complaints concerning the policies and procedures;
- Implement and apply appropriate sanctions against employees who fail to comply;
- Refrain from intimidating or retaliatory acts against any individual for the exercise of any right established under HIPAA Privacy Rule;
- Refrain from requiring an individual to waive his or her rights under HIPAA Privacy Rule, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

In addition, employers may consider revising their business associate agreements to address breach notice obligations and require business associates to reimburse them for all expenses incurred in relation to any breach of unsecured protected health information caused by the business associate. ■

Contacts

LABOR AND EMPLOYMENT LAW

William M. Furr, Chair	wfurr@wilsav.com	757/628-5651
Wm. E. Rachels, Jr.	wrachels@wilsav.com	757/628-5568
Thomas M. Lucas	tlucas@wilsav.com	757/628-5690
Samuel J. Webster	swebster@wilsav.com	757/628-5518
Susan R. Blackman	sblackman@wilsav.com	757/628-5646
David A. Kushner	dkushner@wilsav.com	757/628-5668
Luba I. Seliavski	lseliavski@wilsav.com	757/628-5624
Bryan C.R. Skeen	bskeen@wilsav.com	757/628-5509

EMPLOYEE BENEFITS

James R. Warner, Jr.	jwarner@wilsav.com	757/628-5570
Cher Wynkoop	cwynkoop@wilsav.com	757/628-5581
David A. Snouffer	dsnouffer@wilsav.com	757/628-5678

NLRB - IS RIP VAN WINKLE AWAKENING?

(CONTINUED FROM PAGE 1)

The current General Counsel is Republican-appointee Ron Meisburg, whose term ends in August 2010. The current seated NLRB members are Chair Wilma Liebman, a Democratic appointee (current term ends August 27, 2011) and Republican-appointee Peter Schaumber (term expires on August 27, 2010). Two new Obama nominees are practicing union-side labor lawyers: Mark Pearce from Buffalo, whose practice is limited to representing unions; and Craig Becker, currently Associate General Counsel of the AFL-CIO and the Service Employees International Union (SEIU).

A number of NLRB decisions over the past eight years by the "Bush Board" were hotly contested, with strong dissents by Democrat appointees Liebman and Walsh. Given those strong dissents and Liebman's current leadership of a newly-constituted NLRB, several previously-decided NLRB decisions may be targeted for reversal. A number of those strong dissents came in cases involving employment policies of general application in union-free workplaces, including the following:

Several previously-decided NLRB decisions may be targeted for reversal.

E-mail and Internet Policies – In a 2007 case, the question involved employees' use of the employer's e-mail system. The employer maintained a policy which prohibited employee use of e-mail for all non-job-related solicitations, although the policy permitted employees' personal use of the e-mail system. When the employer enforced the policy and disciplined employees for sending non-work-related but union-related e-mails, those employees filed charges with the NLRB. The NLRB held that employees have no statutory right to use the employer's e-mail system for union or other "protected concerted activity" under the National Labor Relations Act ("NLRA"). Since the company did not permit use of the e-mail system for solicitations for any "outside organizations," the employees were properly disciplined.

Chairman Liebman's strongly-worded dissent characterized the NLRB as the "Rip Van Winkle of administrative agencies," which "has been asleep for the past 20 years…and fails to recognize that…the e-mail system is a piece of communications equipment to be treated just as the law treats bulletin boards, telephones, and pieces of scrap paper." Chairman Liebman would hold that where an employer has given employees access to e-mail for regular, routine use in their work, "we would find that banning all non-work related 'solicitations' is presumptively unlawful absent special circumstances."

Employers may anticipate that when the NLRB now has a case before it presenting the same issue, this precedent will be reversed, and it will become more difficult for employers to prohibit its employees' use of computer systems and e-mails for personal use, including union-related communications.

Employees' Right to a Co-worker "Advocate" in Investigatory Interviews – The NLRB has vacillated for years on the question of whether employees in a non-union workplace have the right to request a co-worker's presence during an investigatory interview that the employee reasonably believes could result in discipline. In 2004, the NLRB ruled that employees have no such right. Chairman Liebman, again dissenting, suggested that the overwhelming majority of employees were being stripped of rights which are integral to workplace democracy.

Employers may expect that in early 2010, unrepresented employees will again be permitted to request the presence of a co-worker in any investigatory meeting or interview which they believe could lead to disciplinary action.

Workplace Rules – Between 2002 and 2005, the NLRB upheld the legality of broad work rules published in employers' disciplinary policies or handbooks. The challenged rules prohibited employee misconduct, including:

- Disloyal, disruptive, competitive or damaging conduct;
- Slanderous or detrimental statements about the employer;
- Representing the employer in a negative manner;
- Abusive or profane language;
- "Fraternizing" with co-workers or employees of a client.

In each case, the NLRB found that the challenged rules were lawful because they served legitimate business interests and would not reasonably be interpreted by employees as interfering with their rights to engage in "protected concerted activity" under the NLRA. Chairman Liebman dissented in each case; she would hold that such rules violate the NLRA because employees might believe that they are not free to communicate with one another about terms and conditions of employment, otherwise "chilling" their exercise of NLRA rights. The new Board may find that rules such as those outlined above are "overly broad" and facially unlawful because they interfere with employees' rights.

The Employee Free Choice Act might not pass Congress and become law. Regardless of whether that Act passes, the exercise of discretion by a newly-constituted NLRB will result in closer scrutiny of workplace rules and will "tip" the balance of such rules in favor of employees and labor unions. We recommend that you review your solicitation/distribution, workplace rules, e-mail/Internet policies, and other workplace policies to ensure that they will withstand closer scrutiny over the next four years. ■

Current and previous issues of the *Employment Law Outlook* are available at: *www.willcoxsavage.com/nep/newsletters.html*.