WILLCOX SAVAGE

Employment Law Outlook

Spring 2015

NLRB FINDS EMPLOYEES HAVE RIGHTS TO USE COMPANY COMPUTER FOR UNION ACTIVITY

William E. Rachels, Jr.

In December 2014, in the case of *Purple Communications, Inc. and Communications Workers of America*, AFL–CIO, Cases 21 CA 095151, 21 RC 091531, and 21 RC 091584, the National Labor Relations Board (the Board or NLRB) ruled by 3-2 that Section 7 of the National Labor Relations Act (the Act) protects the rights of employees to use a company computer and e-mail system for communications regarding self-organization and other terms and conditions of employment. Such ruling is a specific reversal of the NLRB's 2007 decision in *Register Guard*, 351 NLRB 1110 (2007), enfd. in relevant part and remanded sub nom. *Guard Publishing v. NLRB*, 571 F.3rd 53 (D.C. Cir. 2009). In that divided decision, the Board held that employees had no statutory right to use their employer's e-mail systems for Section 7 purposes. It was based fundamentally upon the employer's property rights in the company computers. However, in *Purple Communications*, the Board found that the *Register Guard* decision placed too much importance on employer's property rights and too little on the importance of e-mail as a means of workplace communications. It noted that the Board had failed to adequately protect employee rights under the Act and abdicated its responsibility "to adapt the Act to the changing patterns of industrial life."

The 2014 decision recognized precedent that had found the workplace to be "uniquely appropriate" and "the natural gathering place" for communications about self-organization and other terms and conditions of employment. It noted that the use of e-mail as a common form of workplace communication has expanded dramatically in recent years. Therefore, in balancing the Section 7 rights of the employees and the property and other rights of employers, the Board held that employee use of e-mail for statutory protected communications on *non-working* time must presumptively be permitted by employers who had chosen to give employees access to their email systems.

The Board stated that its decision "is carefully limited." First, it was stated to apply only to employees who have already been granted access to the employer's e-mail system in the course of their work and does not require

(CONTINUED ON PAGE 3)

FMLA "SPOUSE" DEFINITION NOW INCLUDES SAME-SEX MARRIAGES, HOWEVER, . . .

Samuel J. Webster

The Family and Medical Leave Act (FMLA), enacted by Congress in 1993, allows certain eligible employees to take job protected, unpaid leave for various healthcare reasons involving children, spouse, self or parent. Congress later modified FMLA to include qualifying exigencies arising from the employee's spouse, child or parent service in the military. Pursuant to FMLA, DOL has issued implementing regulations, modified from time to time.

The FMLA defines "spouse" as "a husband or wife, as the case may be." 29 U.S.C. § 2611(13). DOL's implementing regulations clarified that the law of the state of the employee's residence would control for determining eligibility for FMLA spousal leave. Since 1995, the FMLA regulations have defined "spouse" as a husband or wife as recognized under the state law where the employee resides ("state of residence" rule).

On a separate front, Section 3 of the Defense of Marriage Act (DOMA) restricted the definitions of "marriage" and "spouse" to male-female relationships, for purposes of federal law, regulations and administrative interpretations, thus limiting the availability of FMLA leave based on a spousal relationship only in heterosexual marriages. 1 U.S.C. § 7. In June, 2013, the United States Supreme Court struck down DOMA's Section 3 as unconstitutional. *United States v. Windsor*, 133 S. Ct. 2675 (2013). Based upon *Windsor*, DOL determined that it was no longer prohibited from recognizing same-sex marriages as a basis for FMLA spousal leave. Prior to *Windsor*, an eligible employee in a legal same-sex marriage who resides in a state that recognizes the employee's marriage could take FMLA spousal leave. However, an employee in a same-sex marriage (from another state) residing in a state that did not recognize same-sex marriages could not take FMLA spousal leave.

DOL began a new rulemaking process in June, 2014, which resulted in a changed definition of "spouse," focusing on the place of celebration of the marriage. The new regulation, effective March 27, 2015, changes the definition of "spouse" to focus on the law of the

(CONTINUED ON PAGE 4)

ANTHEM BREACH - ACTION ITEMS FOR EMPLOYERS

Cher E. Wynkoop and Corina V. San-Marina

On February 4, 2015, Anthem announced that it had been the target of a cyber-attack and the personal information accessed may have included names, health plan identification numbers, dates of birth, addresses (both physical and e-mail), phone numbers, employment information, income data, and Social Security numbers. Since the information accessed qualifies as "protected health information" or PHI under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Anthem, and in many cases employers, have breach notification obligations under HIPAA. Employers, as plan sponsors on behalf of their group health plans, need to identify how the breach may affect them and take appropriate actions. The actions that need to be taken by an employer in response to the Anthem data breach depend on the type of group health plan it sponsors.

Insured Group Health Plan

If the plan is insured, Anthem should be responsible for HIPAA and HITECH compliance and the notification obligation resides primarily with Anthem. Based on Anthem's public communications thus far, it appears that Anthem is proceeding with the mitigation and notice process already.

Self-Insured Group Health Plan

If the plan is a self-insured group health plan and Anthem serves as a third party administrator (TPA), Anthem's legal obligations under HIPAA and state law, as applicable, generally require only that it notify the employer concerning the circumstances of the breach — how it happened, the kind of information breached, who was affected, etc. Then it is up to the employer/covered entity to carry out an appropriate investigation, provide notice to affected individuals and otherwise comply with the applicable federal and state laws. However, administrative service agreements and business associate agreements between employer sponsors and Anthem may delegate notification responsibilities to Anthem as the TPA.

An employer should closely examine its administrative service agreement and "business associate agreement" with Anthem. In particular, the employer should focus on the breach assessment and notice provisions and determine who is responsible for evaluating possible breaches and issuing required notifications to the affected individuals. If the employer retains responsibility to provide the required notice, it needs to determine whose data was compromised, identify the actions required to protect the data and mitigate harm, and prepare the notices necessary to comply with the plan's obligations under HIPAA and state law. HIPAA requires notices be provided without unreasonable delay, but no later than 60 days after the covered entity is informed of the breach by its business associate.

HIPAA requires notices be provided without unreasonable delay, but no later than 60 days after the covered entity is informed of the breach by its business associate.

While Anthem continues its forensic investigation, plan sponsors of a self-insured group health plan should be proactive and consider taking the following actions:

- Ask for written assurances from Anthem that their group health plan and its data were not affected by the recent data breach. If unable to obtain such assurance within a reasonable period of time, it may be safe to assume that the plan was affected.
- If Anthem confirms that the group health plan was affected, confirm that the data breach qualifies as PHI, which in turn would trigger breach notifications.
- Review the service agreements and business associate agreements to determine which party is responsible for HIPAA breach notifications and the impact of any indemnification provisions.
- If Anthem is the party responsible for any HIPAA notifications, coordinate with Anthem representatives so that the notifications provided on your behalf will be sufficient to meet your obligations under HIPAA and state law, if applicable.
- Internally document the actions taken to demonstrate that you are aware that a security incident affecting your group health plan has occurred and your organization is acting in accordance with any written plan policies and procedures.
- Contact your insurance carrier if you purchased cyber insurance coverage or other type of coverage to determine if this type of breach would be covered under the policy.

If you need help in evaluating your risk and developing an appropriate plan of action, contact your legal counsel.■

NLRB FINDS EMPLOYEES HAVE RIGHTS TO USE COMPANY COMPUTER FOR UNION ACTIVITY

(CONTINUED FROM PAGE 1)

employers to require such access in the first place. Second, it was noted that an employer may justify a total ban on non-work use of e-mail, including Section 7 use of non-working time, by demonstrating that special circumstances make the ban necessary to maintain production or discipline (*i.e.*, rebut the presumption against such a restriction). Further, absent justification for a total ban, the employer may apply uniform and consistently-enforced controls over its e-mail system to the extent such controls are necessary to maintain production or discipline. Ultimately, the Board recognized that it did not address e-mail access by non-employees, nor any other type of electronic communications systems since neither such issue was raised in the case.

The particular rules of the employer in issue in *Purple Communications* were contained in its Internet, intranet, voicemail and electronic communication policy. It provided that "All such equipment and access should be used for business purposes only." It proceeded to "strictly prohibit" employees from using such systems and any other company equipment in connection with:

- Engaging in activities on behalf of organizations or persons with no professional or business affiliation with the Company.
- Sending uninvited e-mail of a personal nature.

Effectively, the *Purple Communications* rulings extend non-work time e-mail use to the same parameters previously provided for non-work time "water-cooler" conversations. Moreover, the NLRB's decision does not appear to give recognition to the dynamic reach and effect of e-mail communication. It does not give controlling recognition to the contrast between water-cooler communications among a few employees and the company-wide network for e-mail.

The NLRB remanded the case to the Administrative Law Judge to reopen the record and to provide the parties the opportunity to present evidence relevant to the standard adopted in the Board's decision. However, the employer decided not to submit evidence of special circumstances to rebut the presumption against the validity of its rules. Accordingly, the Administrative Law Judge found that the subject electronic communication policy violated Section 8(a)(1) of the Act, the unfair labor practice for interference with employee rights under Section 7.

The case has been transferred back to the NLRB where it is subject to further review. The NLRB's ultimate decision is subject to appeal to the courts. The outcome will be watched with interest.■

EMPLOYERS BEWARE: EMPLOYEES' SOCIAL MEDIA ACCOUNTS ARE PRIVATE IN VIRGINIA

Phillip H. Hucles

On January 14, 2015, the Virginia General Assembly enacted House Bill No. 2081 codifying a social media privacy law. With the rise in use of social media, many states have enacted social media privacy laws and the Commonwealth of Virginia becomes one of the most recent to enact such a law.

Code of Virginia §40.1-28.7:5, entitled "Social media accounts of current and prospective employees," prohibits an employer from requesting or requiring a prospective or current employee to provide his or her username and password to any social media account. The statute also prohibits an employer from requiring the current or prospective employee to associate or add to their list of contacts the employer on the social media account or to change their privacy settings to allow the employer to view content on their account page.

The statute also includes a retaliation provision, which prohibits an employer from taking any adverse employment action against an employee for engaging in activity protected under the statute.

Notwithstanding these protections, an employer is not liable if it:

- Views information publicly available;
- Inadvertently learns the login/account information and/or accesses the private account; or
- Requests information from the account in conjunction with a formal investigation into employee conduct that may violate state or federal law or an employer's internal policies.

Through normal monitoring policies, employers may gain username and password information of its employees. Although the statute expressly states that an employer does not violate the statute through these actions, an employer may not gain access to the employee's social media account through the information learned on its own devices given to employees or through associated network monitoring.■

WILLCOX SAVAGE
440 Monticello Avenue, Suite 2200
Norfolk, Virginia 23510

FMLA "SPOUSE" DEFINITION NOW INCLUDES SAME-SEX MARRIAGES, HOWEVER, . . .

(CONTINUED FROM PAGE 1)

jurisdiction in which the marriage occurred ("state of celebration" rule). The new rule, 29 C.F.R. § 825.102, assures that all legally married couples, whether opposite-sex or same-sex, will have consistent FMLA rights regardless of where they reside. Thus, if a same-sex couple marries in a state which allows same-gender unions, but works in a state that does not, the employer nevertheless must honor that marriage for purposes of making FMLA spousal leave decisions.

HOWEVER, a Texas Federal district court judge has now stayed enforcement of the new regulation. The court sided with four states (Texas, Arkansas, Louisiana, Nebraska) and enjoined implementation of the "state of celebration" rule. The court held that the new rule requires states to violate full faith and credit laws and to violate state laws that prohibit the recognition of same-sex marriages. The court also found a substantial likelihood that the states would prevail on their claims. So, for now, the "state of residence" rule continues to apply to FMLA spousal leave decisions. **STAY TUNED**.■

CONTACTS

Labor & Employment Law

William M. Furr, Chair	wfurr@wilsav.com
William E. Rachels, Jr.	wrachels@wilsav.com
Gregory A. Giordano	ggiordano@wilsav.com
Samuel J. Webster	swebster@wilsav.com
Christopher A. Abel	cabel@wilsav.com
Susan R. Blackman	sblackman@wilsav.com
David A. Kushner	dkushner@wilsav.com
Stephanie N. Gilbert	sgilbert@wilsav.com
Phillip H. Hucles	phucles@wilsav.com

Immigration

Susan R. Blackman	sblackman@wilsav.com
James B. Wood	jbwood@wilsav.com

Employee Benefits

Cher E. Wynkoop	cwynkoop@wilsav.com
David A. Snouffer	dsnouffer@wilsav.com
Corina V. San-Marina	csanmarina@wilsav.com