December 2014

Weil

Employer Update

Employment Law Implications of Ebola Threat

By Jeffrey S. Klein, Nicholas J. Pappas, and Daniella Adler

As a result of the recent Ebola outbreak in West Africa, many U.S. employers have become concerned about how to address potential exposure to Ebola in the workplace. In this article, we outline some common situations that might arise, and offer guidance and advice based on the operative legal framework. We first describe the background of the recent Ebola outbreak and explain health authorities' pronouncements about how the disease is spread. Next, we examine the specific legal issues employers may face in industries with a higher risk of exposure, when employees travel to areas with widespread Ebola infections, or when employees take adverse action against coworkers based on national origin- or race-based stereotypes. We conclude by offering some practical advice.

In This Issue

Background

The recent Ebola outbreak originated in Guinea and spread to Sierra Leone and Liberia. This outbreak garnered significant media attention in the U.S. when information about a patient with Ebola traveling to the U.S. first surfaced. The Centers for Disease Control and Prevention (CDC) confirmed the Ebola diagnosis on September 30, 2014.[1] About two weeks later, two healthcare workers who cared for that patient contracted the disease themselves. *Id.* On October 23, 2014, the CDC confirmed the diagnosis of a healthcare worker who contracted Ebola in Guinea, sparking additional media coverage. *Id.* In light of these developments, employers have become increasingly concerned about how they might react if their own employees become exposed to the virus.

Ebola Virus Disease, also known as Ebola Hemorrhagic Fever, spreads through direct contact with blood, other body fluids, and skin of people with Ebola symptoms or through contact with the bodies of those who died of Ebola, according to the CDC.[2] Symptoms — including fever, headache, weakness, diarrhea, and unexplained hemorrhage — appear anywhere from two to twenty-one days after exposure.[3]

Ebola can spread, once a person is symptomatic, through coughs, sneezes, and germs left on surfaces, but the CDC has reported no conclusive scientific evidence establishing that Ebola spreads between humans through particles in the air the way "airborne" diseases like tuberculosis and chicken pox do.[4] However, studies on transmission through small airborne particles do not

eliminate that possibility. *Id.* The CDC also stated that the Ebola virus can survive for several hours on dry surfaces and for up to several days at room temperature in body fluids.[5]

Higher Risk Industries

The CDC stated that the risk of contracting Ebola is very low.[6] Despite the CDC's current assessment and the small number of people in the U.S. who have actually contracted the disease, the CDC and other governmental authorities have taken action to study the issue, to inform the public, and to seek to contain the spread of the virus. Employers should heed these developments, particularly in light of the fifty percent death rate in the recent 2014 outbreak.[7]

Employers in industries with an elevated risk of exposure should be most vigilant and prepare to address any sudden case of Ebola that may arise. Employers whose workers may be at higher risk include those in the healthcare, funeral, and airline industries.[8] A threshold concern for such employers is their obligations under the Occupational Safety and Health Act (OSHA), which requires that employers maintain a workplace "free from recognized hazards" that are likely to kill or cause "serious physical harm." *See* 29 U.S.C. § 654.

Employers whose workers may be at higher risk include those in the healthcare, funeral, and airline industries.

To the extent workers in these industries may come into contact with body fluids of people with Ebola, employers should seek to comply with OSHA's bloodborne pathogens standard, which, among other things, directs employers to create and maintain an exposure control plan, to provide protective equipment to potentially exposed employees when warranted at no cost to them, and to store and dispose of "potentially infectious materials" according to regulatory specifications. *See* 29 C.F.R. § 1910.1030.

Employee Travel

Employers who conduct business in countries with widespread Ebola outbreaks also have particularly acute concerns regarding the risk of spreading the virus in the workplace. If an employer requires employees to travel to affected areas for business reasons, those employers should be prepared to respond to opposition from affected employees. Specifically, employers should consider whether employees who refuse to travel to those countries would argue that their opposition constitutes protected activity under OSHA or the National Labor Relations Act (NLRA).

Employees may refuse a task if presented with a choice between serious injury or death and refusing to perform assigned tasks, but only if the employer refuses to correct the hazard, regular enforcement channels would react too slowly, and the employee has "no reasonable alternative."

Under OSHA, employees typically may not refuse to work because of potentially unsafe working conditions. *See* 29 C.F.R. § 1977.12(b)(1). Employees may refuse a task if presented with a choice between serious injury or death, and refusing to perform assigned tasks, but only if the employer refuses to correct the hazard, regular enforcement channels would react too slowly, and the employee has "no reasonable alternative." *See* 29 C.F.R. § 1977.12(b)(2). An employer may not discriminate against an employee for refusing to work in that situation if the employee does so reasonably and in good faith. *See Whirlpool Corp. v. Marshall*, 445 U.S. 1, 19 (1980).

If an employee, in conjunction with other employees, refuses to work because of a perceived risk of

exposure to Ebola, that employee may argue that the NLRA protects that refusal. For example, if an employee suffers adverse action based on a Facebook post[9] about working conditions that the employee believes to be unsafe, that employee may claim that the employer has violated the right to engage in "concerted activities … for mutual aid and protection." *See* 29 U.S.C. § 157.

Employers also should be prepared to deal with employees who choose to travel to affected countries for personal reasons, such as vacations or family visits. An employer may not learn where employees have traveled during personal time off, and even if an employer learns that an employee traveled to a country experiencing an outbreak of Ebola, the Americans with Disabilities Act (ADA) restricts mandatory medical examinations and the types of questions an employer may ask about employee travel.

The ADA prohibits disability-related inquiries and medical examinations unless they are job-related and consistent with business necessity. *See* 42 U.S.C. § 12112 (d)(4)(A). Although the U.S. Equal Employment Opportunity Commission (EEOC) has made no pronouncements on requiring employees to answer questions about potential exposure to the Ebola virus or to undergo medical examinations, the EEOC's guidance released in response to the 2009 H1N1 flu pandemic provides helpful guidelines.[10] The guidance states that a disability-related inquiry or medical examination is "job-related and consistent with business necessity" when an employer "has a reasonable belief, based on objective evidence" that a medical condition will impair an employee's ability to perform essential job functions or that a medical condition causes an employee to pose a direct threat. *Id.* The EEOC also explained that employers may not ask questions that tend to reveal a disability, such as describing a general diagnosis that leads them to take sick leave, but the CDC indicates the employers may ask about whether an employee is experiencing specific symptoms of a disease if it poses a direct threat. *Id.* The EEOC further stated that measuring an employee's body temperature is inappropriate unless the flu pandemic becomes "more severe" or "widespread in the community" according to the CDC or "state or local public health officials." *Id.*

Direct Threat

If an employer learns that an employee has contracted Ebola, the employer may take action to exclude that employee from the workplace. Assuming that an employee is "disabled" under the ADA,[11] the ADA allows employers to require that an individual not "pose a direct threat to the health and safety of other individuals in the workplace." *See* 42 U.S.C. § 12113(b). Four factors determine if an employee presents a direct threat: duration of risk, nature and severity of harm, likelihood of harm, and imminence. *See* 29 C.F.R. § 1630.2(r). The determination must be "based on a reasonable medical judgment that relies on the most current medical knowledge and/or the best available objective evidence." *Id.* A good-faith belief that a significant risk exists is insufficient. *See Bragdon v. Abbott*, 524 U.S. 624 (1998) (holding that doctor did not provide objective evidence supporting refusal to treat AIDS patients in his office).

Stereotypes

Employers also should be prepared to confront irrational stereotypes among coworkers who fear contracting Ebola and who may make irrational assumptions based on improper, unscientific bases. For example, if an employee refuses to work with a coworker from a country with a widespread Ebola outbreak even though that coworker did not visit her home country recently, that refusal would be based on fear and stereotypes. An employer facing that behavior can justifiably take adverse action against the employee who has refused to work based on such irrational fears or stereotypes. Conversely, if an employer fails to discipline an employee acting out of fear and stereotypes, the employer could face claims from the coworker for discrimination. For example, in a case prior to the current outbreak, a court cited a supervisor's comment that he "hoped [a black employee] did not have the Ebola virus that they have over in Africa" as one of the comments that constituted evidence of a hostile work environment of race discrimination. *See Dalton v. Jefferson Smurfit Corp. (U.S.)*, 979 F. Supp. 1187, 1191 n. 4 (S.D. Ohio 1997).

Best Practices

Employers whose employees face a heightened risk of exposure should consider disseminating up-to-date information about Ebola to their employees, informing them of the signs and symptoms of Ebola, the methods of contracting the disease, and reminding them to engage in infection prevention measures like washing hands and using hand sanitizer. Those employers also can adopt a voluntary reporting policy, asking their employees to report any symptoms to the employer, while assuring them that no adverse action will be taken.

By contrast, employers whose employees do not face a heightened risk of exposure to Ebola appear to have little to do immediately, at least presently. Right now, the CDC's admonition that the risk of exposure to Ebola is low appears to be the most relevant information to most employers. Unless and until the number of Ebola cases increases in any employer's places of operation or becomes more prevalent in the U.S., most employers should remain calm and monitor CDC and government pronouncements regarding the spread of the disease and new scientific developments in understanding the illness.

This article was originally published in the New York Law Journal on December 1, 2014.

---

1. *Previous Updates*, Centers for Disease Control and Prevention (Oct. 29, 2014), http://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/previous-updates.html.
2. *Review of Human-to-Human Transmission of Ebola Virus*, Centers for Disease Control and Prevention, http://www.cdc.gov/vhf/ebola/transmission/human-transmission.html (last updated Oct. 29, 2014) (CDC Transmission Review).
3. *Signs and Symptoms*, Centers for Disease Control and Prevention, http://www.cdc.gov/vhf/ebola/symptoms/index.html (last updated Nov. 2, 2014).
4. *See* CDC Transmission Review, *supra* note 2.
5. *Questions and Answers*, Centers for Disease Control and Prevention, http://www.cdc.gov/vhf/ebola/transmission/qas.html (last updated Nov. 20, 2014).
6. *Epidemiologic Risk Factors to Consider when Evaluating a Person for Exposure to Ebola Virus*, Centers for Disease Control and Prevention, http://www.cdc.gov/vhf/ebola/exposure/risk-factors-when-evaluating-person-for-exposure.html (last updated Nov. 28, 2014).
7. *West Africa Ebola Outbreak*, Centers for Disease Control and Prevention, http://www.cdc.gov/vhf/ebola/pdf/west-africa-outbreak-infographic.pdf (last visited Nov. 25, 2014).
8. *Workplace Safety and Health Topics*, Centers for Disease Control and Prevention, http://www.cdc.gov/niosh/topics/ebola (last updated Nov. 21, 2014).
9. *The NLRB and Social Media*, National Labor Relations Board, http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media (last visited Nov. 24, 2014) (explaining that the NLRA protects some social media activity).
10. *Pandemic Preparedness in the Workplace and the Americans with Disabilities Act*, Equal Employment Opportunity Commission, http://www.eeoc.gov/facts/pandemic_flu.html (last updated Oct. 9, 2009).
11. The ADA protects "qualified individual[s]" on the "basis of disability." *See* 42 U.S.C. § 12112. Under the ADA, individuals with disabilities are those who have a "physical or mental impairment that substantially limits one or more major life activities," including anyone "regarded as having such impairment." *See* 42 U.S.C. § 12102. A major life activity can include any major bodily function, including bladder and bowel functions, as well as walking, standing, and concentrating. *See* 42 U.S.C. § 12102(2).

A New Weapon in Combating Employee Trade Secret Theft?: The Discoverability of Personal Emails in Trade Secret Litigation

By Christopher J. Cox, David R. Singh, and Hannah L. Jones

Trade secret theft is an ongoing concern for employers given the high rate of employee mobility in today's workforce. Employee turnover can be rapid – the average employee stays at his or her job for 4.6 years according to the most recent available data from the Bureau of Labor Statistics.[1] With the rate of employee separations continuing to grow, the threat of an employer losing highly valuable trade secrets is real and not a matter of if, but when. Rogue employees often use their personal email accounts to forward valuable information belonging to their employer and believe that this theft will never be discovered. The Stored Communications Act (SCA) is frequently cited by those employees to prevent discovery of content information in those personal emails.

With the rate of employee separations continuing to grow, the threat of an employer losing highly valuable trade secrets is real and not a matter of if, but when.

On October 21, 2014, the California Court of Appeals for the Sixth District issued an opinion which allows an employer, under certain circumstances, to obtain a defecting employee's personal emails directly from the email service provider through discovery in trade secret litigation. In *Negro v. Superior Court (Navalimpianti USA, Inc.)*, 230 Cal.App.4th 879 (Cal. 6th Oct. 21, 2014), the court held that an email account holder's court-ordered consent to the production of his personal emails permits an email service provider to disclose the information in compliance with a civil subpoena without violating the SCA. Thus, under *Negro*, email service providers may no longer invoke the SCA as a blanket immunity from compliance with civil discovery requests. Instead, email service providers may be required to disclose personal email content where the user has provided "lawful consent" to disclosure through a court order.

Importance of Personal Email in Employee Mobility Cases

Savvy employees who are looking to leave their current employers aren't likely to use their work email to discuss new employment. Additionally, on the way out, employees are more likely to use personal email accounts, the cloud, or small personal devices such as flash drives to take proprietary documents and data with them when they leave the company.

Sometimes, the content of an employee's personal email is the only evidence of the misappropriation in a trade secret case. This becomes a problem when the rogue employee refuses to hand over personal emails and/or when the employee has tried to cover his or her tracks by deleting potentially incriminating emails from a personal account. Under either circumstance, the evidence of the theft may only be obtained from the servers of the email service provider. However, an email service provider's ability to disclose the content of personal emails, even when served with a civil subpoena, is limited by the privacy protections of the SCA.

The SCA

The SCA provides that an "electronic communications service" is prohibited from "knowingly divulg(ing) to any person or entity (other than the addressee or intended recipient) the contents of a communication while in electronic storage by that service." 18 USC § 2702(a). The computer systems of an email provider, a bulletin board system or an internet service provider are examples of facilities that provide electronic communication service under the SCA. *In re iPhone Application Litig.*, 844 F.Supp.2d 1040, 1057–58 (N.D. Cal. 2012). The SCA also covers email

messages stored on a server pending delivery or remaining on the server *after* delivery or deletion by the user for "backup protection." *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004). Finally, the SCA does not protect a user's non-content metadata from disclosure (such as the sender, date, and time associated with an email); it only protects the substance of the communication. 18 USC § 2702(c)(6).

An email service provider cannot be compelled to disclose the content of a user's personal email if the disclosure would require the provider to violate the SCA. *See Negro*, 230 Cal.App.4th at 889; *O'Grady v. Superior Court*, 139 Cal.App.4th 1423, 1441 (2006). But there are several exceptions to the statute under which a court may enforce a subpoena and compel disclosure, including disclosures made with the "lawful consent" of a party to the communication. *See* 18 USC § 2702(b)(3) (stating that consent is effective if given by "the originator or an addressee or intended recipient of such communication"). The SCA, however, does not specify the meaning or requirements of the "lawful consent" exception.

Negro v. Superior Court

Negro v. Superior Court resolved the issue of whether a court's order requiring a party to provide consent for an email provider to disclose personal email content satisfied the "lawful consent" exception of the SCA. Under *Negro*, "lawful consent" includes court-ordered consent.

In *Negro*, Matteo Negro (Negro) and other former employees of Navalimpianti USA, Inc. (Navalimpianti), a marine equipment manufacturer, were accused of misappropriating Navalimpianti's trade secrets to start their own competing business. The ship manufacturer sought discovery of emails exchanged between Negro and fourteen other former employees allegedly involved in the conspiracy. The case was venued in Florida.

During discovery, Navalimpianti subpoenaed an email service provider in California, seeking emails from Negro's personal email account which Navalimpianti alleged was used to misappropriate trade secrets and further the conspiracy. The email service provider objected to the disclosure and filed a motion to quash the subpoena in California state court on the grounds that it was prohibited from disclosing the content of the emails under the SCA. Perhaps in response to the email service provider's objection, Navalimpianti obtained an order in the Florida court directing Negro "to execute an Authorization to Release Electronic Communications in a form acceptable to [the email service provider]." The authorization was then sent to the email service provider as directed by the Florida court.

The California Superior Court thereafter denied the motion to quash and directed the email service provider to produce the messages. Negro then filed a petition for writ of mandate with the Sixth District Court of Appeals to set aside the order denying the motion to quash, arguing that the court-ordered consent was not "lawful consent" as required by the SCA. Negro contended that his consent could not be considered "lawful" under the statute because it was both involuntary and judicially coerced.

Under *Negro*, the content of emails is not necessarily immune from civil discovery merely because the emails are kept in a "personal" email account.

The Court of Appeals affirmed the denial of the motion to quash, holding that the court-ordered authorization was "lawful consent" that vitiated the protections of the SCA. The court noted that the "lawful consent" exception to the SCA is not satisfied by consent that is "merely constructive, implied by law, or otherwise imputed to the user by a court." The court reasoned, however, that this does not mean that a court lacks the power to compel the actual consent of a user: "where users are also parties to civil litigation, the court has the means to compel them to give their actual consent. Those

observations came in response to a contention that the SCA cannot have been intended to categorically foreclose the discovery of email messages in civil litigation." Furthermore, according to the court, the consent given by Negro pursuant to a court-order was not judicially coerced and constituted "lawful consent" because Negro was not deprived of volition in complying with the court order – Negro had a choice between providing the authorization and risking discovery sanctions by defying the order. Accordingly, the court held that court-ordered consent is effective to satisfy the "lawful consent" exception to the SCA and permits service providers to make disclosures as required by subpoena.

Practical Implications for Employers

The court's decision in *Negro* provides an additional tool for employers bringing trade secret claims against their former employees, especially where there is reason to believe an employee may have used his or her personal email to misappropriate confidential or proprietary information. Although rights to privacy can still be respected, under *Negro*, the content of emails is not necessarily immune from civil discovery merely because the emails are kept in a "personal" email account. Also, emails deleted locally by the user may still be recovered through a subpoena to the email service provider.

However, caution should be used. *Negro* is the first California opinion on this subject and the California Supreme Court has not addressed this issue.[2] Further, although *Negro* removes an absolute bar on discovering email content through a court order, disclosure is not inevitable given the involvement of a somewhat unpredictable variable: the court must first agree to issue an order requiring the user to give consent.

1. See *Employer Tenure Summary: Employee Tenure in 2014,* Bureau of Labor Statistics (Dec. 2, 2014), available at http://www.bls.gov/news.release/tenure.nr0.htm.
2. As of December 7, 2014, no court outside of California has ruled directly on this issue.

Employer Update is published by the Employment Litigation and the Executive Compensation and Employee Benefits practice groups of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Employment Litigation and Executive Compensation and Employee Benefits practices, please speak to your regular contact at Weil, or to the editors or practice group members listed below:

Editor:

Lawrence J. Baer lawrence.baer@weil.com +1 212 310 8334

Associate Editor:

Millie Warner millie.warner@weil.com +1 212 310 8578

Practice Group Members:

Jeffrey S. Klein
Practice Group Leader
New York
+1 212 310 8790
jeffrey.klein@weil.com

Frankfurt

Stephan Grauke
+49 69 21659 651
stephan.grauke@weil.com

London

Joanne Etherton
+44 20 7903 1307
joanne.etherton@weil.com

Ivor Gwilliams
+44 20 7903 1423
ivor.gwilliams@weil.com

Miami

Edward Soto
+1 305 577 3177
edward.soto@weil.com

New York

Lawrence J. Baer
+1 212 310 8334
lawrence.baer@weil.com

Gary D. Friedman
+1 212 310 8963
gary.friedman@weil.com

Steven M. Margolis
+1 212 310 8124
steven.margolis@weil.com

Michael Nissan
+1 212 310 8169
michael.nissan@weil.com

Nicholas J. Pappas
+1 212 310 8669
nicholas.pappas@weil.com

Amy M. Rubin
+1 212 310 8691
amy.rubin@weil.com

Paul J. Wessel
+1 212 310 8720
paul.wessel@weil.com