FDCC QUARTERLY

VOL. 63, NO. 4 SUMMER 2013

LITIGATION AND SOCIAL MEDIA: USING SOCIAL MEDIA TO YOUR ADVANTAGE AT EVERY STEP OF THE TRIAL
Marisa A. Trasatti and Anna C. Horevay

AVATARS AND SOCIAL MEDIA: EMPLOYMENT LAW RISKS AND CHALLENGES IN THE VIRTUAL WORLD
Michele Ballard Miller

AVATAR IN THE COURTROOM: IS 3D TECHNOLOGY READY FOR PRIMETIME?
Karen L. Campbell, Lauren A. Jones and David B. Datny

WHAT'S IN A NAME(D) STORM? WHAT SANDY HAS TAUGHT US ABOUT FLOOD, STORM SURGE, AND FEMA FLOOD ZONES
Michael K. Kiernan and Michael F. Lenhardt

FDCC QUARTERLY VOLUME 63 INDEX

FEDERATION OF DEFENSE & CORPORATE COUNSEL

FDCC OFFICERS

PRESIDENT
TIMOTHY A. PRATT
Boston Scientifc Corporation
Natick, MA
508-650-8616
timothy.pratt@bsci.com

PRESIDENT-ELECT
VICTORIA H. ROBERTS
Meadowbrook Insurance Group
Scottsdale, AZ
602-445-5920
VRoberts@centurysurety.com

SECRETARY-TREASURER
STEVEN E. FARRAR
Smith Moore Leatherwood LLP
Greenville, SC
steve.farrar@smithmoorelaw.com

BOARD CHAIR
EDWARD M. KAPLAN
Sulloway & Hollis PLLC
Concord, NH
603-224-2341
ekaplan@sulloway.com

EXECUTIVE DIRECTOR
MARTHA (MARTY) J. STREEPER
11812 N. 56th Street
Tampa, FL 33617
mstreeper@thefederation.org
813-983-0022
813-988-5837 Fax

PUBLICATIONS CHAIR
BRUCE D. CELEBREZZE
Sedgwick LLP
San Francisco, CA
bruce.celebrezze@sedgwicklaw.com

FDCC QUARTERLY-EDITOR
SUSAN M. POPIK
38 Woodhill Drive
Redwood City, CA 94061
susan.popik@thomsonreuters.com
650-465-4613
650-362-1890 Fax

EDITOR-FLYER
GREGORY A. WITKE
Patterson Law Firm
Des Moines, IA
gwitke@pattersonfirm.com

SENIOR DIRECTORS

BRUCE D. CELEBREZZE
Sedgwick LLP
San Francisco, CA
bruce.celebrezze@sedgwicklaw.com

WALTER DUKES
Dukes Dukes Keating Faneca PA
Gulfport, MS
walter@ddkf.com

H. MILLS GALLIVAN
Gallivan, White & Boyd, PA
Greenville, SC
mgallivan@gwblawfirm.com

J. SCOTT KREAMER
Baker, Sterchi, Cowden
& Rice, LLC
Kansas City, MO
kreamer@bscr-law.com

DEBORAH D. KUCHLER
Kuchler Polk Schell Weiner
& Richeson, LLC
New Orleans, LA
dkuchler@kuchlerpolk.com

ELIZABETH F. LORELL
Gordon & Rees LLP
Florham Park, NJ
elorell@gordonrees.com

DONALD L. MYLES JR.
Jones, Skelton & Hochuli
Phoenix, AZ
dmyles@jshfirm.com

DEBRA TEDESCHI VARNER
McNeer Highland McMunn
Varner LC
Clarksburg,WV
dtvarner@wvlawyers.com

EDITOR-WEBSITE
DAVID M. FUQUA
Fuqua Campbell, PA
Little Rock, AR
dfuqua@fc-lawyers.com

FDCC HISTORIAN
STEPHEN P. PATE
Norton Rose Fulbright
Houston, TX
stephen.pate@nortonrosefulbright.com

DIRECTORS

ROBERT L. CHRISTIE
Christie Law Group, PLCC
Seattle, WA
bob@christielawgroup.com

EDWARD J. CURRIE, JR.
Currie Johnson Griffin Gaines
& Myers PA
Jackson, MS
ecurrie@curriejohnson.com

ANDREW B. DOWNS
Bullivant Houser Bailey, PC
San Francisco, CA
andy.downs@bullivant.com

MICHAEL T. GLASCOTT
Goldberg Segalla, LLP
Buffalo, NY
mglascott@goldbergsegalla.com

HOWARD M. MERTEN
Partridge, Snow & Hahn
Providence, RI
hm@psh.com

LESLIE C. PACKER
Ellis & Winters, LLP
Raleigh, NC
leslie.packer@elliswinters.com

BRETT J. PRESTON
Hill Ward & Henderson PA
Tampa, FL
bpreston@hwhlaw.com

TODD A. ROBERTS
Ropers, Majeski, Kohn Bentley
Redwood City, CA
troberts@ropers.com

W. MICHAEL SCOTT
CrownQuest Operating, LLC
Midland, TX
mscott@crownquest.com

CLE COORDINATOR
FRANCIE BERG
3714 22nd Avenue South
Minneapolis, MN, 55407
fberg@mahoney-law.com

FDCC QUARTERLY

SUMMER 2013 VOLUME 63, NUMBER 4

CONTENTS

LITIGATION AND SOCIAL MEDIA: USING SOCIAL MEDIA TO YOUR ADVANTAGE AT EVERY STEP OF THE TRIAL
Marisa A. Trasatti and Anna C. Horevay 252

AVATARS AND SOCIAL MEDIA: EMPLOYMENT LAW RISKS AND CHALLENGES IN THE VIRTUAL WORLD
Michele Ballard Miller.....279

AVATAR IN THE COURTROOM: IS 3D TECHNOLOGY READY FOR PRIMETIME?
Karen L. Campbell, Lauren A. Jones and David B. Datny 295

WHAT'S IN A NAME(D) STORM? WHAT SANDY HAS TAUGHT US ABOUT FLOOD, STORM SURGE, AND FEMA FLOOD ZONES
Michael K. Kiernan and Michael F. Lenhardt.....318

FDCC QUARTERLY VOLUME 63 INDEX.....340

Cite as: 63 FED'N DEF. & CORP. COUNS. Q. ___ (2013).

The Federation of Defense & Corporate Counsel Quarterly is published quarterly by the Federation of Defense & Corporate Counsel, Inc., 11812 North 56th Street, Tampa, FL 33617.

Avatars and Social Media: Employment Law Risks and Challenges in the Virtual World†

Michele Ballard Miller

I. Introduction

As if companies and their in-house and outside counsel did not have enough to juggle in today's business and regulatory climate, they must increasingly manage whole new "alternate" or "virtual" universes in the workplace along with the unique legal issues they present. At the same time, most employees are engaged in a host of social media and other online activities, both during the workday and after hours, that can affect their employers and raise additional legal challenges.

This article will examine the risks for employers with this surge in online activity, as well as how far employers can go to regulate and manage such activities. Part II addresses the world of virtual universes and avatars and the risks they pose for employers. Part III examines business risks to employers from employee social media use, including statutory and other limits on an employer's ability to discipline or terminate employees for improper use of social media. In conclusion, Part IV provides practical advice on how employers can manage these risks and minimize potential liability.

---

† Submitted by the author on behalf of the FDCC Employment Section. The author acknowledges and thanks Carolyn Rashby, Special Counsel at Miller Law Group, who assisted with the preparation of this article.

Michele Ballard Miller is a shareholder in Miller Law Group, a 24-attorney firm with offices in San Francisco and Los Angeles that devotes its practice to representing business in all aspects of California employment law and related litigation. With over 30 years' experience practicing exclusively in the area of labor and employment law, Ms. Miller represents management in the full range of litigation, from wrongful termination to sexual harassment to disability discrimination. Ms. Miller also provides strategic advice on employment risk management and is a frequent lecturer on employment issues for clients and outside groups. Ms. Miller currently serves as Chair of the Federation of Defense & Corporate Counsel's Employment Practices and Workplace Liability Section.

II.
Virtual Universes And Employment Risks

A. *Virtual Universes and Avatars: What Are They?*

What is a virtual universe? It is an online community in the form of a simulated environment through which users can interact with one another and with the environment, including using and creating objects. Users take the form of "avatars," which are electronic images that represent and are manipulated by the individual users.[1] The term "avatar" is a Sanskrit word that means the human or animal form of a god on earth.[2] Virtual worlds are sometimes referred to as "synthetic worlds."

Avatars are common in the virtual worlds of online gaming, but also are used in computer conferencing, text-based chat rooms, and similar applications. Some users select avatars that resemble themselves as they are in real life, but they may also choose an alternate form to be their digital persona, be it human, animal, vegetable, mineral, monster, or robot—the only limit is the user's imagination. A user can customize his or her avatar's clothing, hair, personality, age, gender, race, and more. Communication between avatars typically occurs via text chats, visual gestures, and sound.

---

[1] *Avatar,* Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/avatar (last visited Jan. 20, 2014). See also *Avatar,* Second Life, http://secondlife.com/whatis/avatar/?lang=en-US (last visited Jan. 20, 2014).

[2] *Avatar*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/avatar (last visited Jan. 20, 2014).

A well-known, and one of the first, virtual worlds is Second Life, a three-dimensional online world imagined and created by its "Residents." Underlying each Resident—or "resi"—is a real person who represents himself or herself online by an avatar. Residents come from all over the world and number in the millions,[3] with roughly 50,000-60,000 logins per day.

Second Life residents can explore the virtual world (known as the "grid"), meet other residents, socialize, shop, go to performances, ski and swim, work, and participate in just about any type of individual or group activity. Residents can also buy, develop, and trade virtual property and services.[4] The world uses a virtual currency, "Linden Dollars," which can be converted to real U.S. dollars. There are some Second Life entrepreneurs and businesses who are making million dollar (that is, real-world dollar) profits.[5] Users include housewives, artists, programmers, lawyers, firefighters, activists, students, business owners, military personnel, doctors, and employees of all sorts. Second Life also promotes what it calls Second Life Work, which encourages organizational use of the virtual world to conduct business, develop products, or engage in employee recruiting or training—eliminating travel time and costs, while at the same time reducing the company's carbon footprint.[6]

B. *Virtual Universes in the Employment Context*

In the real human resources world, many employers are putting virtual worlds such as Second Life Work or There.com to good use, using these sites to hire employees and conduct new-hire orientations and employee training. Is a hiring manager unable to make it to a job fair across the country? He or she can send an avatar to do the work.[7] Is it time to bring on a new hire in a remote location? The orientation can be conducted in Second

---

[3] Unconfirmed statistics put the current number of Residents at just over 36 million, with about 10,000 to 12,000 new signups per day. Daniel Voyager, *Second Life statistics 2013 winter update*, Daniel Voyager's Blog (Dec. 2, 2013), http://danielvoyager.wordpress.com/2013/12/02/second-life-statistics-2013-winter-update/.

[4] *See, e.g., Introducing Buying Land,* Second Life, http://secondlife.com/land/?lang=en-US (last visited Jan. 20, 2014).

[5] *See* Michael S. Rosenwald, *Second Life's virtual money can become real-life cash*, The Washington Post, (March 8, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/07/AR2010030703524.html. "Nobody in Second Life pays for anything with actual currency. They pay in Linden dollars, which, like real-world currency, is traded on an exchange. Linden Lab, like the Federal Reserve, controls the exchange and money supply to maintain a steady value for Linden dollars. That value has historically hovered around 250 Linden dollars for every U.S. dollar." *Id.*

[6] Linden Lab, *Second Life Work: The Virtual Work Advantage*, http://lecs-static-secondlife-com.s3.amazonaws.com/work/SL-Work-Brochure-010411.pdf.

[7] As a bonus, because the hiring decision can be made without the interviewer ever meeting the applicant in person, the interviewer cannot have access to age, race, disability, and other protected information that can be dangerous in the hiring process.

Life. Companies are also setting up virtual workplaces for employees to meet, hold events, practice corporate communications, conduct training, provide interactive customer service, and more.

But the anonymity and fun/gaming factors that make virtual worlds and workplaces a boon for employers also pose some genuine risks. Among other problems, individuals participating in a virtual world may feel that real-world rules, norms, and laws do not apply.

Recent psychology studies involving virtual world users may provide some insight. A 2010 article in *Psychology Today* posits:

> [The anonymity of virtual worlds] gives the individual the ability to be free from social norms, family pressures or expectations they may face in their personal real world lives. However with this anonymity, other consequences come into play when you look at the commitment aspect of identity formation. For example, if an individual creates a virtual identity that is different from their real life identity, it can take a lot of psychological effort to maintain the false identity. In addition, one of the two options will occur, the identities may converge into one, making the virtual and real identities more true, or the individual may simply toss out the virtual identity, and start over with a new one.[8]

While this anonymity gives users an opportunity to freely explore their identity, it raises some troubling issues of trust for others in the virtual world—namely, "how much, if any, of an individual's virtual identity is *really*—real?"[9] Another study concluded that virtual worlds are a place in which users can "retreat from the painful memories, deficits, and helplessness they experience in the real world."[10] "While in real life individuals hesitate to communicate their true opinions, it is easier to do so online because they don't ever have to meet the people they are talking with."[11]

C. *Virtual Harassment, Bias, and Other Business Risks*

Given these psychological realities, it is not surprising that key employment law risks in the virtual universe include sexual harassment (sometimes referred to as "e-harassment"), bullying, and even assault. For example, someone conducting a job interview in Second Life might harass an existing employee, or vice-versa; a customer might harass one of its

---

[8] Tina Indalecio, *Exploring Identity in the Virtual World–Is that REALLY you?,* Curious Media, April 30, 2010 (citations omitted), http://www.psychologytoday.com/blog/curious-media/201004/exploring-identity-in-the-virtual-world-is-really-you.

[9] *Id.*

[10] Ellen Toronto, *Time Out of Mind: Dissociation in the Virtual World*, 26 Psychoanalytic Psychol. 117, 117 (2009).

[11] *Id.* at 119.

supplier's employees; an employee or a third party might post an offensive image in an organization's virtual world space where it could be viewed by an applicant or another employee during a training session; a male employee might decide to select a curvaceous and buxom female as his avatar. Might an employee offended by these virtual world choices have a hostile work environment claim?

In a May 2006 edition of *Second Opinion*, a former newsletter of Second Life, the creators acknowledged that harassment and assault are common violations in the virtual world,[12] and the site has set "community standards" warning against harassment, assault, and other abuses.[13] Harassing behaviors may include "impeding the free movement of residents, continuous instant messaging or other unwanted contact, and sexual harassment and verbal abuse."[14] Although the harassment may be taking place in an alternate world, it may be very real for an organization's legal purposes.

Another concern is the emerging issue of "virtual bias" stemming from an individual's ability to fashion an avatar that differs from his or her actual appearance. On the one hand, it could be argued that the virtual workplace holds some promise "for leveling the playing field if stereotypes do not manifest in the same negative ways as they have been shown to do in [the] physical work environment."[15] For example, "[a] black male employee who adopts a white male avatar may reap the benefits of the choice to project a different identity."[16] But it is also possible that an employee might complain of discrimination in the virtual world based on his or her "perceived" race, religion, or gender—for example, a white employee who chooses a black avatar and is ostracized in the virtual workplace by coworkers who never met the "real" employee face-to-face. Similarly, a black worker who adopts a white avatar might later complain that he suffered discrimination when his coworkers discovered that his "real" identity did not match the expectations they formed in the virtual work environment.[17]

---

[12] *Police Blotter: Dealing with Harassment in Second Life*, Second Opinion (May 2006), http://web.archive.org/web/20090508045101/http://secondlife.com/newsletter/2006_05/. *See generally* Anthony Curtis, *Second Life and Virtual Worlds: Safeguards for Traveling in Second Life*, http://www.uncp.edu/home/acurtis/NewMedia/SecondLife/SafeguardsInSecondLife.html (last visited Jan. 3, 2014).

[13] *Community Standards*, Second Life, http://secondlife.com/corporate/cs.php (last visited Jan. 3, 2014). For example, the site sets the following community standard regarding harassment: "Given the myriad capabilities of Second Life, harassment can take many forms. Communicating or behaving in a manner which is offensively coarse, intimidating or threatening, constitutes unwelcome sexual advances or requests for sexual favors, or is otherwise likely to cause annoyance or alarm is Harassment." *Id.*

[14] Curtis, *supra* note 11.

[15] *See* Natasha T. Martin, *Diversity and the Virtual Workplace: Performance Identity and the Shifting Boundaries of Workplace Engagement*, 16 Lewis & Clark L. Rev. 605, 626 (Summer 2012).

[16] *Id.*

[17] *Id.* at 627.

Moreover, in virtual spaces, individuals sometimes engage in what is known as "flaming"—i.e., "communication errors such as rude outbursts and other confrontational interaction."[18] The virtual world equivalent of bullying, flaming incidents "can be as equally degrading to a corporate culture as face-to-face conflict."[19]

There are other possible problems, too, stemming either from activities in an organization's private virtual space or from an employee's on- or off-duty activities in a public virtual world space. An avatar could disclose a company's secrets, violate a company's policies, or violate intellectual property laws. A company's dress code could even come into play if, for example, an employee's avatar is scantily or otherwise inappropriately clothed in front of real-world coworkers or clients.[20]

Some organizations have taken a proactive approach to avoiding legal risks in the virtual world. The first to do so was IBM, in 2007.[21] The company's "Virtual Worlds Guidelines for Employees" instruct employees on topics ranging from avatar appearance and etiquette to protecting the company's good name, protecting privacy, handling inappropriate behavior, and respecting confidentiality and intellectual property agreements.[22] These guidelines also make clear that the company's "real world" business conduct rules apply equally to employee behavior in virtual worlds.[23]

III.
Risks of Employee Social Media Use

A. *Business Risks to Employers*

During the workday, employees often spend time "Facebooking" their friends, "tweeting" the latest updates to their followers, or just surfing the web. Though these activities may decrease productivity, they typically do not cause additional harm to the employer. In extreme cases, however, such activities may cause significant harm. For example, employees

---

[18] *Id.* at n.129.

[19] *Id.* at 630.

[20] *See* Ed Finkel, *Will Dress Codes for Workplace Avatars Soon Be the Norm?,* A.B.A. J. (Feb. 1, 2011), http://www.abajournal.com/magazine/article/dress_for_virtual_success/. The article cites an example of a virtual world dress code problem: "Rozwell remembers attending a virtual business meeting in which the host's avatar wore an ostentatious array of jewelry and 'clothing that needed a bit more coverage,' she says. 'That would have been fine if the person were marketing jewelry. But given that this was a software vendor, it didn't jibe well.'" *Id.*

[21] *See* Rachel Konrad, *IBM Writes Guidelines for Virtual World*, USA Today (July 26, 2007, 11:56 AM), http://usatoday30.usatoday.com/tech/webguide/internetlife/2007-07-26-ibm-virtual-guidelines_n.htm.

[22] *IBM Social Computing Guidelines*, IBM, http://www.ibm.com/blogs/zz/en/guidelines.html (last visited Jan. 30, 2013).

[23] *Id.*

may harass their coworkers, reveal confidential company information, endorse products or services without proper disclosure, or engage in criminal conduct. In such instances, employers may face significant risks, including the following:

- *Disclosure of sensitive company information*: Employees may inadvertently (or sometimes intentionally) reveal proprietary or confidential information on a blog, in an email, or on a social networking site. Such privacy breaches, whether malicious or innocent, can be extremely damaging. Consider these examples:
  - In September 2011, a Microsoft executive was fired for tweeting about an upcoming Nokia phone product.[24] His tweets allegedly violated the company's social media policy, which prohibited employees from disclosing new features or products that had not been publicly disclosed without first checking with management.[25]
  - In May 2012, the CFO of Francesca's, a women's boutique chain, was terminated after tweeting about company financials: "Board meeting. Good numbers = Happy Board" and "Roadshow completed. Sold $275 million of secondary shares. Earned my pay this week."[26]
- *Defamation of coworkers or clients*: Employers may face liability for defamation—or cyber slander—based on electronic communications disseminated by employees.[27] Even if the statements are not defamatory, employees can create turmoil by posting rumors, gossip, or offensive statements regarding their coworkers and supervisors. Negative comments by management about a departing employee may also create liability.
- *Harassment and discrimination:* Social networking sites, blogs, and other forms of electronic communication can provide employees with additional avenues for engaging in inappropriate conduct, during work or after hours. Employees may vent workplace frustrations by posting discriminatory statements, racial slurs, or sexual innuendo directed at coworkers, management, customers, or vendors. Such comments may be actionable.

---

[24] Todd Bishop, *Windows Phone manager who tweeted inside info about Nokia device is out at Microsoft*, Geekwire (Sept. 20, 2011, 9:35 AM), http://www.geekwire.com/2011/windows-phone-manager-tweeted-nokia-device-microsoft/.

[25] *Id*.

[26] Rachel Emma Silverman, *Facebook and Twitter Postings Cost CEO His Job*, Wall Street Journal (May 14, 2012), http://online.wsj.com/news/articles/SB10001424052702303505504577404542168061590.

[27] See Thomas J. Mew IV, *Cyber-Defamation: What Is It and How Should Businesses Respond?,* 21 Bus. Torts J. 8 (A.B.A. Sec. Litig., Fall 2013), *available at* http://apps.americanbar.org/litigation/committees/businesstorts/articles/fall2013-1013-cyber-defamation-how-business-should-respond.html.

- *Retaliation:* Comments in cyberspace may also subject the employer to claims of retaliation. For example, after a group of employees filed an overtime action under the Fair Labor Standards Act ("FLSA"), the company owner and director of operations posted the following comments about two of the employees on a blog and on Facebook: "This particular case will end up pissing me off cause it is coming from someone we terminated for theft"; and "Dear God, please don't let me kill the girl that is suing me."[28] The court held that the posts could be deemed retaliatory under the FLSA because they could deter the employees from pursuing their statutory claims.[29]
- *Mandatory reporting requirements:* Some states, including Arkansas, California, Illinois, Missouri, North Carolina, Oklahoma, Oregon, South Carolina, and South Dakota, have mandatory reporting statutes that require information technology workers to report child pornography found on computers they are servicing, and subject the employer to statutory liability if employees fail to comply.[30] (In such cases, employers should also take care to preserve the evidence for legal authorities.)
- *Federal Trade Commission (FTC) guidelines:* According to the FTC Guides concerning the use of endorsements and testimonials in advertising, employers may face liability for unfair competition when employees comment on their employer's services or products on the Internet without disclosing the employment relationship.[31] For example, if an employee endorses his or her employer's product in an Internet post, the statement must be made in compliance with these FTC guidelines—and both the employee and employer face liability if the statement is false or unsubstantiated.[32]
- *Unfair competition laws:* In certain circumstances, use of social media can implicate unfair competition laws. Several recent cases have involved employees' use of LinkedIn. In one case, an IT services and staffing company, TEKsystems, Inc., alleged that three ex-employees (and one current employee) who

---

[28] Stewart v. CUS Nashville, LLC, No. 3:11–cv–0342, 2013 WL 456482, *4 (M.D. Tenn. Feb. 6, 2013).

[29] *Id.* at *11.

[30] *See, e.g.,* Ark. Code § 5-27-604; Cal. Penal Code § 1165.7; 325 Ill. Comp. Stat. 5/4.5; Mo. Rev. Stat. § 568.110; N.C. Gen. Stat. § 66-67.4; Okla. Stat. tit. 21, § 1021.4; S.C. Code Ann. § 16-3-850; S.D. Codified Laws § 22-22-24.18. In addition, the Appellate Division of the Superior Court of New Jersey has held "that an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activity, lest it result in harm to innocent third-parties." Doe v. XYC Corp., 887 A.2d 1156, 1159 (N.J. Super. Ct. App. Div. 2005).

[31] 16 C.F.R. § 255.5.

[32] *Id*.

were bound by noncompetition and nonsolicitation obligations used LinkedIn to unfairly compete against it, including by contacting TEKsystem's contract employees.[33] According to TEKsystems, one of the employees had LinkedIn connections "with at least 20" of its contract employees, and sent them electronic messages inviting them to visit her in her new office.[34] The parties eventually entered into a stipulated order to enforce the nonsolicitation agreement.[35] More recently, a court in Massachusetts concluded that an employee's LinkedIn update regarding a job move was not a prohibited solicitation of business in competition with the former employer, despite the fact that some of the employee's 500 LinkedIn contacts were customers of the former employer.[36] While neither of these rulings provides much guidance as to how to resolve claims involving the interplay between LinkedIn and unfair competition laws, they clearly raise issues to which employers should be paying close attention.

- *Misappropriation of Trade Secrets:* In another recent case, *PhoneDog v. Kravitz*, an interactive mobile news and reviews resource, PhoneDog, sued former employee Noah Kravitz over ownership of a Twitter account, @PhoneDog_Noah.[37] PhoneDog alleged Kravitz was given use of and maintained the account to post product reviews and promote PhoneDog's services to the account's 17,000 followers.[38] Upon termination of his employment, Kravitz changed the Twitter handle to @noahkravitz, but continued to use the account to post to the same followers.[39] PhoneDog sued Kravitz for misappropriation of trade secrets, among other claims, alleging that both the account and its password constituted proprietary, confidential information and that the list of followers was the equivalent of a customer list in which PhoneDog had an intangible property interest.[40] The court refused to dismiss the misappropriation claim, and the case eventually settled, with Kravitz obtaining ownership of the account.[41]

---

[33] TEKsystems, Inc. v. Hammernick, No 0:10-cv-00819, 2010 WL 1624258, ¶19 (D. Minn. Mar. 16, 2010).

[34] *Id.*

[35] *Id.*, 2010 WL 3514960 (Sept. 3, 2010).

[36] KNF & T Staffing, Inc. v. Muller, No. 13-3676-BLS1, 2013 WL 7018645, *3 n.5 (Mass. Super. Ct. Oct. 24, 2013).

[37] No. C 11-0374 MEJ, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).

[38] *Id*. at *1.

[39] *Id*.

[40] *Id.* at *4.

[41] *Id.* at *6-7.

B. *Disciplining Employees for Misusing Technology*

There are myriad scenarios that may prompt an employer to discipline an employee for the misuse of technology and social media. The most obvious is when an employee engages in illegal conduct while at work. But what if the unlawful conduct occurs outside of work? Or if an employee engages in on-duty behavior that is legal, but the employer finds troublesome, annoying, or damaging? Consider these examples:

- Music retailer HMV received unwanted publicity when the company's online marketing and social media planner "live tweeted" a layoff as it was occurring.[42] "We're tweeting live from HR where we're all being fired! Exciting!!!" "There are over 60 of us being fired at once! Mass execution, of loyal employees who love the brand. #hmvXFactorFiring." "Just overheard our Marketing Director (he's staying, folks!) ask 'How do I shut down Twitter?'"[43]

- An Applebee's waitress posted on a social media site a photo of a receipt on which a customer had written: "I give God 10%. Why do you get 18?" [44] The customer's signature/name was legible in the post.[45] The waitress was terminated for violating Applebee's social media and privacy policies, which prohibited employees from transmitting internal information or posting identifying information about customers on social media sites. The post and its aftermath, however, caused "viral mayhem."[46]

- Two former employees of Houston's restaurant in Hackensack, N.J., sued in federal court after they were fired for criticizing the restaurant on MySpace.[47] They set up a private MySpace forum specifically as a forum to vent about work, and emailed invitations to coworkers.[48] A supervisor called a coworker into his office and obtained her login information; that information was then passed on to higher-level supervisors, who used it to log in to the forum and view the comments.[49] The plaintiffs contended that the employer's unauthorized access to the forum violated the federal Stored Communications Act, as well as their

---

[42] Harry Bradford, *HMV Employee Hijacks Company Twitter Account Amid 'Mass Execution' Layoffs*, Huffington Post (Jan. 31, 2013, 12:14 PM), http://www.huffingtonpost.com/2013/01/31/hmv-twitter-hijacked_n_2591227.html.

[43] *Id*.

[44] *Waitress Fired for Posting Note About Tip*, USA Today (Feb. 1, 2013, 7:46 PM), http://www.usatoday.com/story/news/2013/02/01/tip-god-waitress-fired/1884961/.

[45] *Id*.

[46] *Id.*

[47] Pietrylo v. Hillstone Restaurant Group, No. 06–5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

[48] *Id*.

[49] *Id*. at *3.

right to privacy under New Jersey law.[50] A key issue was whether Houston's management properly obtained access to the site using the login information it obtained from the coworker, or whether the employee was coerced into revealing the information.[51] The result was an $18,000 verdict against the company, which included an award of punitive damages for "malicious" conduct.[52]

Before taking disciplinary measures against an employee based on the use or misuse of social media or technology, employers should consider whether there are legal constraints preventing or limiting such action. Generally, it is not illegal to look at an employee's public blog, Facebook page, or YouTube video. But, as the Houston's restaurant dispute shows, accessing a private site without permission raises serious legal issues. And as HMV and Applebee's learned, even if a company is acting lawfully when it disciplines or terminates a worker, the negative publicity that may follow can cause the company even more damage than the employee's initial post.

Even if an employer learns about an employee's online activities or conduct legally, there may be restrictions on what the employer can do with the information and limitations on what actions the employer can take against the employee. Laws that may apply include:

- *National Labor Relations Act ("NLRA")*: The NLRA affords all employees the right to engage in "concerted activity," including the right to discuss the terms and conditions of employment affecting the employee and coworkers.[53] Thus, before disciplining an employee who, for example, has complained about the employer on Facebook, an employer should determine if the employee has engaged in protected concerted activity.[54]
- *Off-duty statutory protections:* Some states, including California, Colorado, Connecticut, New York, and North Dakota, have enacted statutory protections for employees who engage in lawful off-duty conduct.[55] For example, the California statute makes it illegal to demote, suspend, or discharge an employee for

---

[50] *Id.* at *1.

[51] *Id.*

[52] *Id.* at *4-6. For other cases with similar content, *see, e.g.,* Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417 (S.D.N.Y. 2010); Maremont v. Susan Fredman Design Group, Ltd., No. 10 C 7811, 2011 WL 6101949 (N.D. Ill Dec. 7, 2011); Rene v. G.F. Fishers, Inc., 817 F. Supp. 2d 1090 (S.D. Ind. 2011).

[53] 29 U.S.C. §151 *et seq.*

[54] The Office of the General Counsel of the NLRB has issued a series of reports examining Board decisions that involved the interplay between the NLRA and employer social media policies and employee discipline. *See The NLRB and Social Media*, NLRB, http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media (last visited Jan. 3, 2014).

[55] *See, e.g.,* Cal. Lab. Code § 96(k); Colo. Rev. Stat. § 24-34-402.5; Conn. Gen. Stat. § 31- 40s; N.Y. Lab. Code § 201-d; N.D. Cent. Code § 14-02/4- 03.

lawful conduct occurring during nonworking hours away from the employer's premises.[56] Some off-duty protection laws contain an exception for material conflicts of interest, allowing an employer to take action if the employee's otherwise lawful conduct harms the employer.[57]

- *Password privacy laws:* A number of states have enacted legislation that prohibits employers from requesting or requiring employees and applicants to disclose their login information for personal social media accounts.[58]
- *Whistleblower laws:* Many federal and state statutes contain protections for employees who reveal corporate wrongdoing. Examples include the Sarbanes-Oxley Act,[59] the Occupational Safety and Health Act,[60] the American Recovery and Reinvestment Act,[61] and the Dodd-Frank Wall Street Reform and Consumer Protection Act.[62]
- *Political activity laws*: In some states, including California, Missouri, Nevada and New York, laws prohibit employers from interfering with an employee's political activities.[63] The Nevada law, for example, provides that it is unlawful for an employer to make any rule or regulation prohibiting or preventing an employee from engaging in politics.[64]
- *Wage disclosure laws*: Some states have enacted laws prohibiting employers from disciplining employees for disclosing or discussing their wages.[65] Taking adverse action in this context might violate the employees' right to participate in concerted activity under the NLRA.[66]

---

[56] Cal. Lab. Code § 96(k). *See also* N.Y. Lab. Code § 201-d(2); N.D. Cent. Code § 14-02.4-01.

[57] *See, e.g.*, N.Y. Lab. Code § 201-d(3); N.D. Cent. Code § 14-02.4-01.

[58] *See, e.g.*, N.J. Assembly Bill No. 2878 (2013); Nev. Assembly Bill 181 (2013); Colo. Rev. Stat. § 8-2-127. The National Conference of State Legislatures tracks legislation regarding employer access to employee social media usernames and passwords. A list of states that have adopted such laws can be found at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

[59] 15 U.S.C. § 1514A.

[60] 29 U.S.C. § 660(c).

[61] Pub. L. No. 111-5, § 1553, 123 Stat. 115, 297-302 (2009).

[62] 15 U.S.C. § 78u–6(h).

[63] *See, e.g.*, Cal. Lab. Code §§ 1101-1102; Mo. Rev. Stat. § 115.637; Nev. Rev. Stat. § 613.040 *et seq.*; N.Y. Lab. Code § 201-d.

[64] Nev. Rev. Stat. § 613.040 *et seq.*

[65] *See, e.g.*, Cal. Lab. Code § 232(a)(b).

[66] See *supra* text accompanying notes 53-54.

- *Constitutional and statutory right to privacy:* The right to privacy afforded by the U.S. Constitution does not apply to private employers. But a state's constitution may apply more broadly, extending privacy protection to private employers and employees.[67] Privacy concerns are most likely to arise when an employer gains unauthorized access to communications the employee believes to be private (e.g., by pretending to be someone else).[68]

  A recent case illustrates how courts analyze privacy rights in the social media context. In *Roberts v. CareFlite,* the plaintiff, a paramedic employed by CareFlite, posted on Facebook that she "wanted to slap" a patient who had needed restraints for transport.[69] In response to a request by CareFlite's compliance officer, plaintiff removed the post, but only after a follow-up post stating that sometimes "a patient needs an attitude adjustment."[70] CareFlite ultimately fired the plaintiff, and she sued for invasion of privacy.[71] The court upheld summary judgment for CareFlite, finding that the plaintiff made no argument and produced no evidence supporting her contention that the employer's actions amounted to an intrusion on her privacy.[72]

  - *Free speech protections:* The First Amendment right to free speech does not apply in a purely private workplace, but some related state laws may apply to private employers. For example, Connecticut law prohibits retaliating against employees for exercising their free speech rights.[73] Some state constitutions also contain free speech protections.[74]

  - *Discrimination and retaliation:* Under federal law and in most states, it is illegal to discriminate on the basis of a protected classification, such as race, gender, disability, or religion.[75] Some states prohibit sexual orientation

---

[67] *See, e.g.*, Cal. Const. art. I, § 1.

[68] *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858 (Ct. App. 2009). In that case, a Coalinga high school posted a negative article about her city and school on MySpace, which the school principal found and submitted to a local newspaper for publication. *Id.* at 861. The student sued the newspaper and the principal, claiming invasion of privacy. *Id*. at 860. The appellate court upheld the sustaining of defendant's demurrer without leave to amend because the facts contained in the article were not private, and the author publicized her opinions by posting the article online. *Id.* at 862-64. *See also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); *supra* text accompanying notes 47-53.

[69] No. 02–12–00105–CV, 2012 WL 4662962 (Tex. App. Oct. 4, 2012).

[70] *Id.* at *1.

[71] *Id.*

[72] *Id.* at *5.

[73] Conn. Gen. Stat. § 31-51q.

[74] Cal. Const. art. I, § 2; Haw. Const. art. 1§ 4; N.J. Const. art. I, § 6.

[75] *See, e.g.*, 42 U.S.C. § 2000e *et seq.*; Cal. Gov't Code § 12940(a).

discrimination.[76] Employers also need to be aware of the anti-retaliation provisions of these laws,[77] particularly in the context of taking action against employees who use online media to oppose an unlawful practice.

The bottom line is that unless an employee's online activities are illegal—or, though legal, are directly harmful to the employer's business or a clear violation of company policy—taking adverse action against the employee poses a high degree of legal risk with minimal benefit. At a minimum, such adverse action is likely to subject the employer to unwanted media scrutiny or negative public attention. Thus, although there is rarely a clear answer on how to proceed in this developing area of the law, the best course of action in many cases will be employer self-restraint.

IV.
Conclusion:
Tips to Avoid Potential Liability

A. *Avoiding Employment Risks in the Virtual World*

Given the risks detailed above, employers should exercise caution with respect to the use, and potential misuse, of the virtual universe. At a minimum, employers should consider the following as a means of protecting their business and legal interests in the virtual universe:

1. Let employees know that inappropriate behavior online is as serious as inappropriate behavior in the "real world," and that all company policies—anti-discrimination, anti-harassment, confidentiality, etc.—will apply. Employees should be required to report all inappropriate work-related behavior to the employer and any service provider (if the conduct is by a third party).
2. Educate employees about intellectual property and confidentiality issues and the prohibitions on disclosing such information in a virtual world.
3. Instruct employees not to disclose personal information about any other employee in a virtual world.
4. Require employees to obtain company authorization before conducting business on the organization's behalf in a virtual world or before purporting to speak or act for or on behalf of the organization.
5. Require that both the appearance and conduct of an employee's avatar be appropriate to the business activity involved. Depending on the circumstances, employees may want to require that employees use business-only avatars rather than personal avatars.

---

[76] *See, e.g.*, Cal. Gov't Code § 12940(a); Mass. Gen. Laws. Ann. ch. 151B, §4(1).

[77] *See, e.g.,* Cal. Gov't Code § 12940(g); Mass. Gen. Laws. Ann. ch. 151B, §4(4).

B. *Minimizing Risks Arising out of Employees' Use of Social Media*

Finding an appropriate balance in connection with employee social media activity is admittedly difficult. Nonetheless, the following steps will help the employer avoid problems:

1. Have a clear written policy regarding Internet and social media use and employee online communications, both inside and outside the workplace. The policy should:
   - Instruct employees that they should refrain from engaging in inappropriate or unacceptable online conduct and clearly define what conduct is proscribed;
   - Remind employees that social media postings are public and generally available for all the world to see;
   - Advise employees to use their best judgment and exercise personal responsibility when posting on social media;
   - Specify that harassing, discriminatory, obscene, pornographic, and malicious conduct on social media is unacceptable and will not be tolerated; and
   - Prohibit employees from divulging the employer's confidential information and trade secrets and require compliance with nondisclosure and confidentiality obligations. To avoid potential conflicts with the NLRA, the policy should define what is meant by confidential information and trade secrets.
2. Require employees to sign an acknowledgment of receipt of the social media policy.
3. Periodically review the policy to ensure it is up-to-date and consistent with the latest legal developments regarding social media use.
4. To avoid unfair competition issues, consider prohibiting employees from uploading work-related contacts or customer or employee lists to their LinkedIn or similar accounts, and state explicitly that the employer owns content, screen names, and passwords associated with work-sponsored social media accounts. For work-related social media accounts, such as those on LinkedIn, consider requiring employees to make their contact lists private.
5. As in all other cases, caution managers not to discipline or terminate an employee for an alleged social media violation without thoroughly reviewing the facts and circumstances and without considering carefully the legal issues that may be implicated.
6. Before taking action, consider whether the employee's activity may be protected, including evaluating whether the employee was speaking as a whistleblower or in some other protected capacity. If action is contemplated, be sure that

the company can articulate specific, substantial harm to the employer and/or workplace from the employee's social media activity.

7. Never circumvent privacy tools or use a false identity to gain information from or access to an employee's private social media pages.

The Federation of Insurance Counsel was organized in 1936 for the purpose of bringing together insurance attorneys and company representatives in order to assist in establishing a standard efficiency and competency in rendering legal service to insurance companies, and to disseminate information on insurance legal topics to its membership. In 1985, the name was changed to Federation of Insurance and Corporate Counsel, thereby reflecting the changing character of the law practice of its members and the increased role of corporate counsel in the defense of claims. In 2001, the name was again changed to Federation of Defense & Corporate Counsel to further reflect changes in the character of the law practice of its members.

The FEDERATION OF DEFENSE & CORPORATE COUNSEL QUARTERLY, published quarterly through the office of publication by the Federation of Defense & Corporate Counsel, Inc., 11812 North 56th Street, Tampa, FL 33617.

Manuscripts and correspondence relating to the submission of articles for possible publication should be sent to the Editor-in-Chief, Susan M. Popik, 15760 Ventura Blvd., Encino, CA 91436 or emailed to susan.popik@thomsonreuters.com. All other correspondence should be directed to the Executive Director.

The FDCC is pleased to provide electronic access to Quarterly articles from 1997 to present at its Internet website, www.thefederation.org.