



**REGULATING EMPLOYEE INTERNET ACTIVITY
OFF-SITE AND OUT OF THIS WORLD**

Michele Ballard Miller
Miller Law Group
111 Sutter Street, Suite 700
San Francisco, California 94104
415.464.4300
www.millerlawgroup.com

As if companies – and their counsel, in particular – did not have enough to juggle in today’s tough business climate, there are whole new “alternate” or “virtual” universes to manage, and they come with their own unique legal issues. What’s more, employees are increasingly engaging in a whole other host of online activities, such as blogging, posting on social networking sites, uploading videos to YouTube and more. This paper 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, even when employees engage in them after hours.

1. The Risks of Virtual Universes

What is a virtual universe? One of the most popular, Second Life, is a 3D online, virtual world imagined and created by its “Residents.” Underlying each Resident is a real person who represents himself or herself online by an “avatar.” Residents number in the millions, come from all around the world, and logged 124 million user hours in the first quarter of 2009, an increase of 42 percent from the same quarter last year.¹

According to *Wikipedia*, “Residents can explore, meet other residents, socialize, participate in individual and group activities, and create and trade virtual property and services with one another, or travel throughout the world, which residents refer to as the grid.”² The world uses a virtual currency, called “Linden Dollars,” which can be converted to real U.S. dollars. There are some Second Life entrepreneurs and businesses that are making million-dollar (that is, real-world dollar) profits.³ Users include housewives, artists, programmers, lawyers, firefighters, activists, students, business owners, military personnel, doctors -- and your employees and colleagues.

¹ The Second Life Economy - First Quarter 2009 in Detail, <https://blogs.secondlife.com/community/features/blog/2009/04/16/the-second-life-economy--first-quarter-2009-in-detail> (last visited May 26, 2009).

² Second Life, http://en.wikipedia.org/w/index.php?title=Second_Life&oldid=292217583 (last visited May. 26, 2009).

³ *Id.*

In the real human resources world, many employers are putting virtual worlds, whether Second Life or similar sites such as There.com, to good use, such as for hiring and conducting employee training and new-hire orientations. Your hiring manager can't make it to the job fair? No problem, just send an avatar to do the work. What's more, many companies view virtual worlds as the ultimate nondiscriminatory medium. For example, hiring can occur without ever actually meeting the applicant, so the interviewer does not have access to age, race, disability and other information about the candidate that can be dangerous in the hiring process anyway.

But the anonymity and fun/gaming factors that makes virtual worlds a boon for employers also pose some genuine risks, particularly because individuals participating in a virtual world may feel that real-world rules do not apply.

One of the key risks in the virtual universe is sexual harassment or assault. This could be a candidate harassing an existing employee, or vice-versa. Or, an employee or a third party might post an offensive image in your organization's virtual world space where it could be viewed by an applicant or another employee during a training session.⁴ Indeed, in a May 2006 edition of

⁴ A recent example is the "pink penis attack" that occurred during a Second Life chat show event hosted by CNET, a technology news site. The chat show was hacked and the guest, Ailin Graef, a popular and successful Second-Lifer who had managed to alienate many users, was continually "attacked" by floating pink phalluses. A video of the attack was quickly uploaded to YouTube, and

Second Opinion, a newsletter of Second Life, the creators acknowledged that harassment and assault are the two most common violations in the virtual world.⁵ Harassing behaviors may take the form of excessive instant messaging, verbal abuse, and other unwanted contact, as well as impeding the movement of avatars. Although the harassment may be taking place in an alternate world, it may be very real for your organization's legal purposes.

There are other possible problems, too, stemming either from activities in your 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 your company's secrets, violate company policy, or violate intellectual property laws.

Some organizations are taking a proactive approach to avoiding legal risks in a virtual world. The first to do so was IBM. In 2007, Big Blue issued "Virtual Worlds Guidelines for Employees," instructing 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.

news of the incident spread quickly across the Internet. (YouTube swiftly removed the offending video when Graef's husband sent the company a Digital Millennium Copyright Act complaint.)

⁵ Dr. Anthony Curtis, Safeguards for Traveling in Second Life, <http://www.uncp.edu/home/acurtis/NewMedia/SecondLife/SafeguardsInSecondLife.html> (last visited May 28, 2009).

Here are five best practices for protecting your company's interests in the virtual universe:

1. Educate employees about intellectual property and confidentiality issues and the prohibitions on disclosing such information in a virtual world.
2. Instruct employees not to disclose personal information about any other employee in a virtual world.
3. Let employees know that inappropriate behavior online is as serious as inappropriate behavior in the "real world" and that all company policies – such as EEO, harassment, confidentiality, etc. – will apply, and all inappropriate behavior that is work-related must be reported to the company and to the service provider (if the conduct is by a third party).
4. Require employees to obtain company authorization before conducting business on the organization's behalf in a virtual world, or if it may appear as if the employee is speaking or acting for or on behalf of the organization.
5. Require that an employee's avatar be appropriate to the business activity involved and, depending on the circumstances, that the employee use a separate business-only avatar rather than his or her personal avatar.

2. Blogs, Social Networking and YouTube: Can You Regulate Off-Duty Internet Activity?

Blogs, YouTube, Twitter, MySpace, Facebook, Second Life. The online possibilities for social networking and other online activities are almost endless, and most of your employees are probably participating to some extent: blogging about their personal and professional lives and uploading photos and videos of themselves.

Most online activities and postings are harmless. But suppose an employee's posting is damaging to your organization, employees or clients, such as by disclosing sensitive information or containing comments that are defamatory, harassing or portray your organization in a negative light. Or maybe the content simply is offensive and not in line with your corporate values, even though your organization is not identified in any way. Consider these recent examples:

- Two former employees of Houston's restaurant in Hackensack, N.J., have filed a lawsuit in federal court after they were fired for bad-mouthing the restaurant on MySpace. They set up a private MySpace forum specifically as a forum to vent about work, and emailed invitations to co-workers. A supervisor called a co-worker into his office and asked for the login information, she handed it

over, and that information was passed on to higher level supervisors, who logged in and viewed the comments. Houston's alleges that the online postings violated company policies on professionalism and having a positive attitude. The plaintiffs contend that the employer's unauthorized access to the forum violated the federal Stored Communications Act⁶ as well as their right to privacy under New Jersey law. A key issue in the litigation is whether Houston's management properly obtained access to the site with the login details it obtained from the co-worker, or whether the employee who revealed the login information to management was coerced into doing so.⁷

- A former Delta Air Lines flight attendant filed a lawsuit for sex discrimination after she was fired for posting (mildly suggestive) photos of herself in Delta uniform on her blog.⁸ She claimed that Delta had not taken similar action against male employees who engaged in similar conduct.

What are the legal parameters for snooping on an employee's off-duty Internet activities, or taking action against employees for such activities? Generally, it is not illegal to look at an employee's public blog or YouTube video,

⁶ 18 U.S.C. § 2701 et seq. (2008).

⁷ See Dionne Searcey, *Employers Watching Workers Online Spurs Privacy Debate*, WALL ST. J., April 23, 2009 at A13.

⁸ *Simonetti v. Delta Airlines Inc.*, No. 5-cv-2321 (N.D. Ga. Filed 2005) (stayed pending Delta bankruptcy proceedings).

for example. But, as the Houston's restaurant dispute shows, accessing a private site without permission could raise serious legal issues.

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

- *National Labor Relations Act.* Blogging or other online comments about one's employment may be protected under the National Labor Relations Act (NLRA) if the commentary or other online activity concerns terms and conditions of employment affecting the employee *and* co-workers. Note, too, that such activity is protected even if the employment is non-union.
- *Off-duty statutory protections.* Some states, such as California, Colorado, Connecticut, New York and North Dakota, have enacted statutory protections for employees who engage in lawful off-duty conduct. For example, the California statute makes it illegal to demote, suspend, or discharge an employee for lawful conduct occurring during non-working hours away from employer's premises.⁹ Some off-duty protection laws contain an exception for

⁹ CAL. LABOR CODE § 96(k) (West 2008). See *also, e.g.*, N.Y. LABOR CODE § 201-d; N.D. CENT. CODE § 14-02.4-01.

material conflicts of interest, such that an employer could lawfully take action if the employee's conduct harms the employer, even if the conduct is otherwise lawful.¹⁰ (The California statute does not contain that exception.) In addition, some states may recognize a public policy violation for terminating an employee for engaging in lawful conduct (such as speech) outside the workplace.

- *Constitutional right to privacy.* The right to privacy in the federal constitution does not apply to private employers. However, some state constitutions, like California's, have broader protections that do extend to private employers and employees. Privacy concerns are most likely to arise when the employee believes the Internet site is private (for example, because it is password-protected), the site promotes itself as private, and the employer gained unauthorized access to the site or used other questionable means of gaining access (such as by pretending to be someone else).¹¹
- *Free speech protections.* Again, the First Amendment right to free speech does not apply in the private workplace, but some state constitutions do apply to private employers. For example,

¹⁰ See, e.g., N.D. CENT. CODE § 14-02.4-01.

¹¹ See *Moreno v. Hanford Sentinel, Inc.*, 172 Cal.App.4th 1125 (App. Ct. 2009) (Coalinga high school student who posted a negative article about her city and school on MySpace brought an invasion of privacy action against a newspaper and the high school principal, after the principal submitted the article to the newspaper and it was published. The court concluded that defendants' demurrer to the invasion of privacy cause of action was properly sustained without leave to amend because the facts contained in the article were not private and the author publicized her opinions about Coalinga by posting the article online). See also *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

Connecticut law prohibits retaliating against an employee for exercising free speech rights,¹² and some state constitutions contain free speech protections, although many of these are limited to the public employment context.¹³

- *Discrimination and retaliation.* In most states and under federal law it is illegal to discriminate on the basis of a protected classification, such as race, gender, disability or religion. Some states prohibit sexual orientation discrimination. Employers also need to be aware of the anti-retaliation provisions of these laws, particularly in the context of taking action against an employee who uses online media to oppose an unlawful practice.
- *Whistleblower laws.* Many federal and state statutes contain protections for employees who blow the whistle on corporate wrongdoing. Examples include the Sarbanes-Oxley Act, the Occupational Safety and Health Act, and the recent American Recovery and Reinvestment Act.
- *Political activity laws.* Some states, including California, Missouri, Nevada, and New York have laws that prohibit employers from interfering with an employee's political activities. The Nevada law, for example, provides that it is unlawful for an employer to make

¹² CONN. GEN. STAT. § 31-51q.

¹³ See *Tucker v. Journal Register East*, No. 3:06CV00307 (D. Conn. Nov. 7, 2007).

any rule or regulation prohibiting or preventing an employee from engaging in politics.¹⁴

- *Wage disclosure laws.* Finally, some states have enacted laws prohibiting an employer from disciplining an employee for disclosing or discussing his or her wages. Note, too, that taking adverse action in this context could also amount to a violation of the NLRA, depending on the circumstances.

The bottom line is that unless an employee's online activities are illegal,¹⁵ or may be legal but are directly harmful to your business or a clear violation of company policy, taking adverse action against the employee poses a high degree of legal risk with minimal benefit to the employer. There's also the consideration that adverse action will subject the employer to unwanted media scrutiny. Unfortunately, there is rarely a clear answer on the best course of action in this developing area of the law. Thus, in many cases, employer self-restraint should be considered.

¹⁴ NEV. REV. STAT. § 613.040.

¹⁵ Consider the recent example involving two Domino's Pizza employees in North Carolina who filmed a "prank" video in the kitchen of the Domino's shop where they worked – the video showed the employees preparing sandwiches while one put cheese up his nose and mucus on the sandwiches. Then, they posted the vignette on YouTube. The workers have claimed it was only a joke, but they have lost their jobs and are facing felony food-tampering charges. See Stephanie Clifford, Video Prank at Domino's Taints Brand, N.Y. TIMES, April 16, 2009 at B1.

Here are suggestions for avoiding problems and finding a legal balance in connection with employee off-duty blogging and other online activities:

1. Adopt a blogging policy that puts employees on notice that it is a violation of company policy to reveal confidential or proprietary information or to disparage other employees, customers or clients.
2. Do not gain unauthorized access to password-protected sites or other areas that are intended to be private.
3. If you do learn about online activity that may be inappropriate or unprofessional, consider ignoring it. By responding, you might be drawing public attention to comments or behavior that might otherwise go largely unnoticed. There is also the employee relations angle to consider. Too much interference by an employer could make employees fearful that they are being spied on when they are off-duty, and that could spur valued workers to leave.
4. Ask an employee to modify the content of an online posting, including removing any information that identifies your organization.
5. When disciplining, focus on the effects on an employee's job performance or violations of company policy, but check state laws before taking action.



Michele Ballard Miller

With more than 25 years of experience practicing exclusively in the area of labor and employment law, Ms. Miller provides strategic advice to companies on a wide range of employment issues. She also defends companies in litigation involving claims of discrimination, harassment, retaliation and other employment-related disputes.

Named a "Super Lawyer" by *Super Lawyers - Northern California* magazine each year since 2004, Ms. Miller is a frequent lecturer on employment issues both for firm clients and outside groups. Her articles on employment issues affecting employers and HR professionals have appeared in numerous publications, on sites and in training materials.

Ms. Miller is on the board of directors of the National Association of Minority and Women Owned Law Firms (NAMWOLF) and is a member of the Federation of Defense and Corporate Counsel (FDCC) as well as the employment law sections of a variety of bar associations.

Ms. Miller received her J.D. from the University of California, Hastings College of Law, in 1982 and her Bachelor of Arts degree from the University of Michigan in 1978.