

EXPERT ANALYSIS

Gamification in the Workplace and Its Impact on Employee Privacy

By Paul Cowie, Esq., and Jessica Fairbairn, Esq.
Sheppard Mullin LLP

Cult movies featuring disgruntled workers, like “Office Space,” “Clerks” and “Horrible Bosses,” and vast rooms filled with silent cubicles are familiar aspects of our popular culture.

A recent Gallup study found that only 30 percent of American employees say they feel “engaged” at work, while 70 percent of employees say they are “not engaged” or are “actively disengaged.”¹ The same study said widespread employee disinterest not only affects company performance, but costs the U.S. economy an estimated \$450 billion to \$500 billion each year.²

But companies such as Bunchball Inc. and Badgeville are looking to change that statistic through gamification, the application of game theory and design to other areas of activity to increase engagement.

Rajat Paharia, founder and chief product officer at Bunchball, says that while some categorize gamification as the use of “points, challenges, awards, leader boards, avatars and badges,”³ the real point of gamification is “to motivate people through data.”⁴

At its most basic, gamification means to design a product, service or operation so the user becomes more engaged and has been used in the consumer context for many years to increase customer loyalty and engagement. McDonald’s Monopoly promotional game is a well-known use of gamification in the consumer context.⁵

Now, gamification is increasingly making its way into the workplace to stimulate employee engagement — and early case studies demonstrate that the application of gamification has resulted in increased employee productivity, efficiency and innovation.⁶ Most recently, T-Mobile rolled out Bunchball’s Nitro platform embed within Jive software to help engage its 30,000 customer service representatives.⁷

Regardless of the form of gamification an employer chooses to implement, the byproduct is almost always large amounts of data about employees performance and work product,⁸ the data that have been used to create leader boards, track individual or team performance or reward high-performing employees.⁹ Consequently, it is important to take precautions to protect the data and employee information gathered.

INTERNAL SHARING OF EMPLOYEE DATA BY THE EMPLOYER

Some gamification applications, particularly those that publicize employee job performance on leader boards or publicly award badges or prizes, by their very nature involve the sharing of employee data throughout the workplace. Employers using such gamification techniques must be cognizant of their employees’ privacy rights when deciding what employee data to publish.



Gamification means to design a product, service or operation so the user becomes more engaged. It has been used in the consumer context for many years.

California employees' right to privacy in the workplace is rooted in the California Constitution, the common law and various privacy-related statutes. California courts have long recognized claims for invasion of privacy in cases where information about the employee was shared. In one case the employer posted a memo in an employee break room detailing the specific reasons for a former employee's termination.¹⁰ In another, the employer announced during a managerial meeting that an employee would be disciplined and was required to draft her own letter of discipline.¹¹

It is easy to see how the courts, when applying these cases to gamification, might likewise find a breach of privacy if an employer publishes information about an employee's work performance through a leader board broadcasting employee rankings.

While the leader board itself may be acceptable, an employer could encounter problems with how it uses the leader boards. For example, an employer that adopts a policy of disciplining the lowest-ranked employee would, in essence, be announcing to the entire workforce that a particular employee will be disciplined when the majority, if not all, of the workforce has no compelling need for the information.

A leader board posting under these circumstances is akin to a memo posted in a common area publicizing the reason for an employee's discipline.¹² It is also not unlike an employer verbally announcing an employee's discipline in the presence of other company managers who had no interest in the matter.¹³ So a court could find a privacy violation.

Informed employers can protect against these risks.

In most workplace privacy claims the employee must demonstrate a *reasonable expectation* of privacy, with which the employer interfered.¹⁴

While is an open legal question whether an employee has a reasonable expectation of privacy in his or her job performance when directly compared to other employees (that is, whether this information would be considered "private" or "confidential"), there are steps an employer can take to manage this expectation.

Before implementing a gamification application that will publish information about an employee's job performance, employers should provide all employees with *clear, written notice* detailing exactly what information the application will gather and what information will be shared with other employees. In cases where employers monitored employees' personal computer use at work, courts have found that whether an employee had an expectation of privacy could depend on how clear the employer's notice about the restrictions on computer usage was.¹⁵ So it is important for employers to pay close attention to the language of their notices.

While not unlike the approach many employers have taken to protect their ability to monitor employees' use of the Internet and email, gamification presents additional challenges because the data will not only be viewed by management, but will often be shared with peers.

Therefore, in addition to providing employees with clear, written notice of the data that will be gathered and shared through a gamification program, employers should also ask their employees to affirmatively *consent* to the gathering and sharing of their information. Because it diminishes the employee's expectation of privacy, consent is a common defense to most privacy claims.¹⁶ So it is prudent for employers to require employees to sign "terms of the game" acknowledging and agreeing to the data-gathering and -sharing aspects of the gamification program *before implementation*.

Courts will not always be satisfied there was not privacy violation, though, simply because an employer obtained the employees' consent, because courts allow employees to consent only to "intrusions that are reasonable under the circumstances."¹⁷ Not all data disclosures can be waived. For example, it is unlawful for an employer to publically post or display employees' Social Security numbers, and employees cannot waive the protection.¹⁸ Employers also have an obligation to protect employees from identity theft.¹⁹ These are all factors to be considered during the gamification project design phase.

EXTERNAL SHARING OF DATA: GAMIFICATION IN SOCIAL MEDIA

Employers embarking on a gamification solution should also address privacy issues that might arise from publishing data outside the workplace. As in any competitive environment, employees using workplace gamification applications, where results might be displayed in leader-board fashion, may be inclined to boast about their achievements, including by posting on Facebook, Twitter, LinkedIn or another social media platforms.

Bragging might be a good indication that the employer's gamification application is working, demonstrating that the employee is engaged in the competition and striving to improve performance, but could also lead to unforeseen consequences. For example, an employee could post a screenshot of the application's leader board to Facebook to announce that he or she is the top performer in the office. This screenshot, though, would also likely reveal the rankings for other employees and could disclose proprietary or confidential information like sales or marketing strategies.

Again, however, all of these risks can be managed through appropriate and robust policies.

Social media policies: Why are they important?

Because social media have become a ubiquitous part of the business world and most individuals' personal lives, it is crucial for employers to implement and enforce policies that clearly outline permissible and impermissible employee conduct on social media websites.

The policies typically say when an employee can and cannot communicate through social media on behalf of the company and set out standards for the communications. They also typically instruct employees on prohibited social media conduct, like posting harassing, discriminatory or retaliatory comments.

The social media risk

Although it is prudent for employers to implement and enforce social media policies, recent decisions demonstrate the need to be exercise care in developing the policies.

The National Labor Relations Board has scrutinized many social media policies to determine whether they violate federal labor law in unionized and non-unionized workforces alike. In less than one year, the NLRB issued three separate general counsel reports describing 35 cases involving social media policies.²⁰ The NLRB found the vast majority unlawful because they were overbroad and could reasonably be construed by employees to restrict "protected concerted activity."²¹

To determine whether conduct constitutes "protected concerted activity," the NLRB looks to whether the activity is concerted, whether it benefits other employees and whether it is carried out in a way that causes it to lose protection.²² Because most employees on a social networking site are connected to at least some of their colleagues, the NLRB is likely to interpret prohibiting employees from posting about gamification as unlawfully restricting the right to engage in protected concerted activity.²³

For example, the NLRB found one social media policy unlawful because it instructed employees not to "release confidential guest, team member or company information."²⁴ The NLRB found the language could be construed to prohibit employees from "discussing and disclosing information regarding their own conditions of employment, as well as the conditions of employment of employees other than themselves" — activities that are protected by the National Labor Relations Act.²⁵ Under this analysis, a social media policy that prevents employees from discussing or disclosing the work performance of other employees via leader board screenshots, for example, might be interpreted by the NLRB as overbroad and unlawful.

Unfortunately, the NLRB has rejected the use of a "savings clause," a blanket statement that the policy is not intended to restrict protected concerted activity, to cure otherwise unlawful provisions in a social media policy.²⁶

Employers using gamification techniques like leader boards to track individual or team performance must be cognizant of their employees' privacy rights when deciding what employee data to publish.

It is prudent for employers to require employees to sign "terms of the game" acknowledging and agreeing to the data-gathering and -sharing aspects of the gamification program before implementation.

As a result, employers may not be able to prevent all the types of communications they want to, particularly where employee-performance information and confidential or proprietary company information intersect. Depending on how an employer's gamification application is designed, leader boards, badges or other awards might reflect precisely this type of "hybrid" information, which is difficult, if not impossible, to keep from being disclosed.

Therefore, employers should keep the foregoing restrictions on social media policies in mind when designing and engineering a gamification application. For example, an employer should be cognizant of how its employees can broadcast the information captured by the application. Employers should also identify what confidential or trade secret information is embedded within the gamification application, and consider whether there is a risk of external publication.

The NLRB decisions underscore the importance of a well-drafted social media policy to protect the employer's confidential, proprietary or trade secret information in the gamification context.

Managing the risk

The good news is that, as with most employment laws, appropriate advice at the design stage of the gamification program helps reduce the risks. The key is to consider these issues and draft policies before implementing the gamification program. Depending on the complexity of the gamified solution, it might be prudent to build the policies into the gamification application itself by providing employees with reminders regarding disclosure of information and, possibly, check boxes to confirm consent to its use. While an employer could attempt to circumvent employee privacy concerns in other ways, such as by displaying only *team* performance rankings, using a team-based approach could also reduce the effectiveness of the gamification program by limiting the ability to motivate individuals through data specific to them. However, these are all considerations for the design phase.

CONCLUSION

Gamification comes with exciting and tangible rewards for employers, but also comes with the responsibility to protect employee privacy. To manage these risks, employers interested in implementing gamification platforms should obtain professional advice to ensure they take all necessary precautions to protect the privacy of their employees, and the confidential information of their company.

NOTES

¹ Gallup Inc., *State of the American Workplace: Employee Engagement Insights for U.S. Business Leaders* (2013), available at <http://www.gallup.com/strategicconsulting/163007/state-american-workplace.aspx>.

² *Id.* at 4-5.

³ Mark van Rijmenam, *Gamification Is The Friendly Scout of Big Data*, BIG DATA STARTUPS, Apr. 19, 2013, available at <http://www.bigdata-startups.com/gamification-is-the-friendly-scout-of-big-data/> (describing the game elements often used in gamification as "points, challenges, awards, leader boards, avatars and badges").

⁴ Interview with Rajat Paharia, Founder and Chief Product Officer, Bunchball Inc. (Aug. 29, 2013).

⁵ See Guy Krief, *How Gamification Can Drive Levels of Consumer Engagement*, MOBILE MARKETER, Aug. 10, 2011, available at <http://www.mobilemarketer.com/cms/opinion/columns/10671.html>.

⁶ Adena DeMonte, *Badgeville.com, Improving Employee Engagement with Gamification*, (June 7, 2013), available at <http://badgeville.com/2013/06/07/improving-employee-engagement-with-gamification>; e.g., William Ng, *Gamification Enters Employee Engagement*, INCENTIVE, Mar. 30, 2011, available at <http://www.incentivemag.com/Incentive-Programs/Engagement/Articles/Gamification-Enters-Employee-Engagement/>; Jim Tierny, *Gamification Key Trend in Employee Engagement and Rewards*, LOYALTY360, Apr. 14, 2013, available at <http://loyalty360.org/resources/article/gamification-key-trend-in-employee-engagement-and-rewards>; Lauren Simonds, *Can Games Drive Productivity?*, TIME, July 22, 2013, available at <http://business.time.com/2013/07/22/can-games-drive-productivity/>.

⁷ *Bunchball Announces Enhanced Gamification Tools for the Jive Platform*, MARKETWIRED, Apr. 8, 2013, available at <http://www.marketwire.com/press-release/bunchball-announces-enhanced-gamification-tools-for-the-jive-platform-1776120.htm>.

⁸ Rijmenam, *supra* note 3.

⁹ The Gates Foundation used a leader-board-style gamification application that tracked their “Social Media Superstars” by measuring social media activity and expertise. The purpose of the leader board was to encourage employees to participate in social media training, and as a result employees increased their social media activity and expertise. See, Leaderboarded, Customer Examples, Leaderboarded.com, available at <http://www.leaderboarded.com/home/customer-examples/> (quoting Tyler Lepard of the Gates Foundation).

¹⁰ *Payton v. City of Santa Clara*, 132 Cal. App. 3d 152 (Cal. Ct. App., 1st Dist. 1982).

¹¹ *Operating Eng’rs Local 3 v. Johnson*, 110 Cal. App. 4th 180 (Cal. Ct. App., 1st Dist. 2003).

¹² *Payton*, 132 Cal. App. 3d 152.

¹³ *Operating Engineers*, 110 Cal. App. 4th 180.

¹⁴ *Hill v. NCAA*, 7 Cal. 4th 1, 32-37 (1994); *Shulman v. Group W Prods.*, 18 Cal. 4th 200, 232 (1998).

¹⁵ *TBG Ins. Servs. Corp. v. Super. Ct. (Zieminski)*, 96 Cal. App. 4th 443, 451-452 (Cal. Ct. App., 2d Dist. 2002); *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979).

¹⁶ *Hill*, 7 Cal. 4th at 40.

¹⁷ *Sheehan v. S.F. 49ers Ltd.*, 45 Cal. 4th 992, 1001 (2009).

¹⁸ Cal. Civ. Code §§ 1798.85(a), 1798.86; 42 U.S.C. § 408(a)(8).

¹⁹ Cal. Civ. Code § 1798.82(a).

²⁰ Nat’l Labor Relations Bd., Report of Acting General Counsel Concerning Social Media Cases (Aug. 18, 2011); Nat’l Labor Relations Bd., Report of Acting General Counsel Concerning Social Media Cases (Jan. 24, 2012); Nat’l Labor Relations Bd., Report of Acting General Counsel Concerning Social Media Cases (May 30, 2012).

²¹ Also referred to as “Section 7 activity” and “concerted activity.”

²² The NLRB has launched a separate website that provides examples of conduct found to be protected concerted activity, <http://www.nlrb.gov/concerted-activity>.

²³ The NLRB’s position is that blanket prohibitions against posting “confidential” or “private” employee information are unlawful because they could be construed to prohibit communications about wages or other working conditions, discussions the NLRB has long permitted. NAT’L LABOR RELATIONS BD., REPORT OF ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES 4 (May 30, 2012).

²⁴ *Id.*

²⁵ *Id.* Section 7 of the National Labor Relations Act protects an employee’s right to “engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.”

²⁶ *Id.* at 11.



Paul Cowie (L) is a partner in the labor and employment group with **Sheppard Mullin LLP** in Palo Alto, Calif., and can be reached at (650) 815-2648 or at pcowie@sheppardmullin.com. **Jessica Fairbairn** (R) is an employment associate in the firm’s San Francisco office and can be reached at (415) 774-3126 or at jfairbairn@sheppardmullin.com.