

Monitoring Employee Behavior

Written by Bruce Metge, Senior Vice President and General Counsel

Digex Incorporated

November 2003

Monitoring Employee Behavior

Here is some earthshaking news: the law is not settled in its view of the internet. As lawyers, we are still learning the meaning and impact of the internet in our lives, and especially the lives of our corporate clients. The internet has a palpable impact on both daily corporate routines and on those high drama events that occasionally consume our lives in dealing with employee matters. As detailed below, because the law is unsettled and internet events tend to move quickly, it is important to establish appropriate policies and procedures relating to the daily routines to put the company in position to address the crises. This paper addresses some of the more significant current issues related to daily routines and crises.

I. Monitoring Employee Communications

Typically, there are three reasons to monitor employee use of company technology: first, to measure the impact of the internet on employee productivity, second, to detect and prevent violations of law within the company, and third, to protect the company's intellectual property.

While the measurement of employee productivity through internet use is an interesting sociological issue, in reality it is little more than an elaborate (if involuntary) time card system, unless it also focuses on the substance of the use itself. The issue then becomes not how much are they doing it, but what are they doing. Then the two most interesting areas are 1) violations of law or the company code of conduct and 2) the taking of company property, discussed below.

At first blush, one wonders why companies would be involved in detecting and preventing possible violations of law. This is one of the cornerstones of law enforcement, and law enforcement would seem to be an odd occupation for most companies. But since the advent of the Federal Sentencing Guidelines, and now with Sarbanes-Oxley and its underlying regulations, it must be concluded that companies are now a part of the mainstream of law enforcement. The cost of ignoring this conclusion is quite high. So a company's right and indeed duty to police employee behavior on the internet must be made clear to employees, because a company has little choice. The ostrich no longer has any place in company management. A company must police employee behavior to prevent wrongdoing by its employees through the use of company systems.

There are additional considerations that firms should take into account in the protection of intellectual property. To understand why monitoring internet use within a company is important, the ease of stealing intellectual property through the internet must be compared with the procedural and systemic bulwarks that a company must overcome to protect its intellectual property.

A proprietary interest in intellectual property is essentially a form of monopoly over that property. In some cases that interest takes the form of a government granted right for a period of time, over an idea, process, or invention that is necessary or useful in the company's business. With respect to the time period, it is worth noting that even a period of months or a year or so may be immensely valuable in the current commercial environment. Intellectual property includes patents, trademarks or copyrights issued by a governmental entity, as well as know-how, proprietary processes, lists, and other

intangibles that are valuable in a company's business. Intellectual property resides in people, papers, computers, and items that can be reverse-engineered or easily transmitted over the internet.

There is a natural skepticism about proprietary intellectual property that arises from several sources. The antitrust laws are wary of intellectual property for the simple reason that the antitrust laws have a bias against monopolies. Second, courts do not like to restrict individuals, and the enforcement of intellectual property rights may involve restricting individual conduct or freedom of speech. Third, there is an academic bias against ownership of intellectual property. It runs contrary to the concept of teaching and free flow of knowledge. This may seem to be a narrow obstacle, but many creative people come from academia, not the business world. Fourth, competition and competitors don't like intellectual property—if it is valuable, then someone out there will be thinking about how to take the value without taking the property, at a minimum. Any or all of these underlying concepts may come into play in specific instances of attempting to protect a company's proprietary interest in intellectual property.

The procedural steps involved in pursuing the taking of a company's proprietary intellectual property are not trivial. First, the company must obtain the intellectual property—someone has to have the idea—which then resides in the minds of people, and usually in written form. Second, there must be evidence of ownership of the property—for this reason alone, it is important to consider government sanction in the form of copyright, trademark or patent. Third, the company must establish internal protections to prevent the intellectual property from being EP—everyone's property. This may be especially important for some types of protective actions, such as actions under the

federal Economic Espionage Act, 18 U.S.C. 1831 et.seq. Fourth, there must be policing to determine whether the company's intellectual property rights are being violated. Unfortunately, one of the most frequent sources of violations is a present or former employee. Fifth, there must be a demand that the violations cease. Sixth, if the demand fails, the company must resort to litigation. Seventh, the company must be successful in the litigation in a timely fashion, or settle favorably. In short, the protection of intellectual property isn't easy, and it isn't cheap.

To protect the company's intellectual property, you must aggressively establish and maintain the foundational protections to be able to monitor behavior on the company's systems. The most important thing the company can do to leave itself free to monitor internet use is to establish, maintain and enforce an appropriate electronic communications policy. The policy should establish that all property used in connection with the company communications system belongs to the company. It should set forth the restrictions on the use of that system, including limitations on content. The policy should cross reference and be integrated with the company code of conduct and record retention policies. But most of all, it should make clear that employees do not have an expectation of privacy in their use of the system, and that violations of the policy may lead to disciplinary action, including termination.

In addition to establishing, maintaining and enforcing appropriate policies, there are some practical steps companies can follow to protect itself from misuse of the communications systems.

1. In setting up internal protections, recognize that this is a cultural issue, not just a legal one. Your company should try to establish a morality of aspiration in the protection of company property, not just a morality of duty.
2. Move carefully but quickly in reaction to potential violations—Organization process can slow pursuit to where its value is diminished, legally and practically.
3. Push your client on the value of maintaining systems to protect company property. Without proper and properly enforced procedures, the company may not be able to pursue misuse of company property.
4. Be a practical voice in protecting company property and pursuing its misuse. For example, in some circumstances, enforcing appropriate restrictive agreements against a departing employee may be much more expensive, more time consuming and less successful than convincing them to stay. In others, retaining the employee might be the worst thing to do. There is no substitute for the exercise of practical good judgment.

II. Unusual email events

If an employee uses company systems in furtherance of a violation of law or, in particular, to steal company intellectual property, a company must take steps to intercede. But what happens when the impropriety of the use is less clear? What happens, for example, when an employee becomes adversarial to the company and sends emails through the company email system or another internet-enabled vehicle to complain to other employees, make his or her views known and enlist support against the company?

Let's assume that the email communications, setting aside their merits, are completely one-sided, vexatious, highly opinionated, and say unfair things about nice people, including the company CEO. Other employees have a variety of reactions to these communications. At a minimum, productivity suffers.

What is the risk of doing nothing? Sometimes the best answer is to monitor and wait. Sometimes these email tornadoes are merely storms in a glass of water, and are best left to dissipate. However, we are all familiar with the combustible danger of bad email. Because it takes no time, no effort and no forethought to distribute an email, an email can create problems very quickly. And because emails are so easily and perfectly repeatable, they tend to garner more credibility than the spoken word. If an email contains false information, the forwarding of an email is a republication of that false information. An email can easily and quickly be leaked to the press, giving the company a public relations issue. It does not take a very vivid imagination to follow the thread to shareholder complaints, whistleblower problems, questions about accuracy of filings, market concerns, shareholder lawsuits, federal and state agency inquiries, or congressional inquiries. And, assuming that the information is easily shown to be false, these matters are difficult enough in their diversionary impact on key people at the company. If the communications contain even a kernel of grossly misportrayed truth, however, the results can be debilitating to the business of the company.

What should counsel do?

1. Study the communications. A careful study of the communications is hugely important. It should include a consideration of the sender, his or her circumstances, the object of the email, the breadth and depth of the distribution of

the communication, a possible profile of the recipients, the content of the email, the accuracy of the information contained in the email, the possible source of the information, the timing of the emails related to other events at the company and so forth,. To do this properly, the company will need to have an appropriate and effective email policy in place, which allows for review of employee email.

2. Make a threshold determination: Is this a serious issue? If so, then create an appropriate internal investigation structure to learn about the issue in a protected environment.
3. Gather all facts underlying the communications. Make an initial determination if there have been possible violations of law, including: Interference with prospective economic relations, Guillory v. Godfrey, 286 P.2d 474, 476-477 (Cal. Ct. App. 1955); interference with contract, Blender v. Superior Court of Los Angeles County, 130 P.2d 179 (Cal. Ct. App. 1942); intentional infliction of emotional distress, Kisesky v. Carpenters' Trust for So. California, 192 Cal. Rptr. 492, 495-497 (Cal. Ct. App. 1983); or other speech based torts, Southridge Capital Mgmt. v. Lowry, 188 F. Supp. 2d 388, 394-396 (S.D.N.Y. 2002).
4. Analyze the merits of the communications. If they have merit, i.e., the company has an instance or a practice that needs to be addressed or modified, then address it.
5. Determine whether there are potential violations of your code of conduct. Even if there are some underlying constructive aspects to the communications, there may still be problems with the emails that need to be addressed. If there are violations of the code of conduct, refer them to the appropriate group in the company to

address them—usually human resources. In addressing the violations, care should be taken to measure them against other situations the company has dealt with, and to carefully analyze how discipline should be handled.

6. Determine whether there is the possibility of continued communications, and advise the company as to the risks of taking steps to minimize or stop those communications. Such steps might include disciplinary action against a current employee, blocking a former employee from sending email to current employees, or court-based injunctive relief against third parties.
7. Alert the company public relations department to the possibility of activity resulting either from the email or from actions taken by the company in response to the email.
8. Give careful consideration to meeting with the sender of the email. The decision whether to communicate with the sender will depend on the results of 1 through 6 above.

What are some of the risks of bringing suit against the individual sending the communications? Consider what happened in Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003). The facts were summarized by the court as follows: On six occasions over almost two years, Hamidi, a former Intel employee, sent emails criticizing Intel's employment practices to numerous current employees on Intel's email system. [Hamidi created the recipient address list using an Intel directory on a floppy disk anonymously sent to him.] Hamidi breached no computer security barriers in order to communicate with Intel employees. He offered to, and did, remove from his mailing list any recipient who so

wished. Hamidi's emails to individual Intel employees caused neither physical damage nor functional disruption to the company's computers, nor did they at any time deprive Intel of the use of its computers. The contents of the messages, however, caused significant disruption and time spent among employees and managers discussing the messages.

Intel sued Mr. Hamidi for trespass to chattel, seeking injunctive relief.

The result? The court held that the injury of disruption of the business resulting from the emails was not the type of injury intended to be protected by trespass. Thus, under Intel Corp. v. Hamidi, it is possible that a former employee can obtain a company email list and send messages to company employees that are highly provocative, negative to the company and individuals at the company, even incendiary, and the company has no action in trespass to chattels for the former employee's use of the company email system.

Assume that your company, faced with a comparable situation, now takes the lesser step of blocking the former employee out of the company email system. The former employee has a friend who is incensed by the company's actions. The friend goes to a public web-based chat board about your company and sends out a series of emails. He calls your upper management incompetent. He suggests that your employees start a rebellion. When contacted by your company to stop, he engages in disassociated chat about guns and bullets with names on them. He accuses the company of racketeering, solicits information to provide to federal prosecutors, and demands jail time for the

company's top officials. The company demands that you bring suit on behalf of the company for intentional interference with contract, intentional interference with prospective economic advantage and unfair business practices, and injunctive relief to cease the harmful communications. After advising the client of the risks, you bring the suit.

What is the likely result? It is possible that the company may lose an anti-SLAPP motion, not obtain an injunction, and be forced to pay the defendant's legal fees for a substantial portion of the defense of the interference claims. In Airborne Express, Inc. v. Moore, 2003 Cal. App. Unpub. LEXIS 7033 (Cal. Ct. App. July 23, 2003), Mr. Moore was the friend of an independent contractor who provided ground delivery services for Airborne. He did not like how his friend was being treated, and began a chat board campaign to complain about Airborne's activities in a very incendiary way. Eventually, Airborne sued Mr. Moore, alleging two counts of tortious interference and one count of unfair business practices. Mr. Moore brought an anti-SLAPP motion against Airborne's claims, and won the motion as to the interference claims. The Airborne decision is an unpublished decision decided in the California Appeals court in July. A petition for review was filed on September 3, so we have not heard the last of this case.

What conclusions can be drawn from these recent cases? Unfortunately the primary conclusion is that these issues are by no means settled today, and companies will continue to be subjected to the uncertainties of their rights to their own systems, even as they will be held accountable for the misuse of those systems. These cases also make it clear that legal action taken by a company against an individual related to communications over the internet must be very carefully considered. These actions may

not turn out the way the company expects. At a minimum, counsel must be careful to advise the company of the many possible outcomes from bringing such actions.

Bruce F. Metge
Senior Vice President and General Counsel
Digex, Incorporated