



## Social Networking Or Social Not-working?

**Wavecrest Computing**  
101 Ocean Park Ave.  
Melbourne, FL 32901  
Toll-free: 877-442-9346  
Voice: 321-953-5351  
Fax: 321-953-5350

[www.wavecrest.net](http://www.wavecrest.net)

Social networking in the workplace is a major dilemma for today's businesses. The question is: "Does it help or hurt the organization?" After reviewing key aspects of the issue, the author – an analyst with Wavecrest Computing – offers some thoughts on solutions.

At Wavecrest Computing, we've been helping businesses and other organizations deal with Internet usage issues for more than twelve years. In *general*, these entities all face the same challenge, i.e., how can the organization maximize the benefits of Internet access while minimizing the risks of personal surfing at work?

Although the general issue is always the same, the *specific* challenges vary. They range from productivity losses, to legal risks, to bandwidth drains and security problems. And even *more* specifically, these challenges are associated with various *types* of sites that employees often visit for personal reasons. A few years ago, pornography sites presented the greatest challenge, while today social networking sites seem to be "number one."

In many ways, the challenge of social networking at work is even greater than that presented by pornography and other inappropriate sites. Why? Because social networking is not "all bad."

Let's explore 'the good and the bad' a bit.

As just about everyone knows, social networking is the "latest thing" – in homes, schools and workplaces. And it is super popular. I'll even bet that most of you readers engage in it—at home, on the road, at work, or maybe even all three.

And it's growing by leaps and bounds:

*"Overall, U.S. visits to social networking Web sites rose 62 percent from September 2008 to September 2009, according to Hitwise, which tracks 155 such sites."*

*"Social technologies continue to grow substantially in 2009. Now more than four in five US online adults use social media at least once a month, and half participate in social networks like Facebook." (Source: Forrester.com)*

Facebook alone has more than 300 million users.

So why such astounding popularity? Two reasons. One is 'personal,' and the other is 'business.'

On the personal side, social networking makes it very easy to satisfy a powerful human need, i.e., association and communication with other human beings. That *can* be a good thing. We are – after all -- 'social animals.'

On the business side, "Web 2.0" computing – which includes social networking – is gradually being used for more and more commercial purposes, especially collaboration. Some managers and analysts believe that it is an excellent way for businesses and other organizations to 'network' with customers, colleagues and partners.

As suggested, these *can* be (repeat, *can* be) good things.

On the other hand, social networking has a serious down side. On a personal level it is so appealing that it can easily be overdone, sometimes to the point of addiction. As a result, parents worry about their kids spending too much time doing it (with attendant risks and behavior issues), and employers worry about its negative impact on their organizations if used for personal reasons.

While parental concerns are certainly important, this article focuses on the latter topic, i.e., social networking in the *workplace*.

At Wavecrest Computing, we live in the world of Internet usage in the workplace. As a result, we are often asked for our thoughts and recommendations on all aspects of the subject, including social networking. So we thought we'd share some of our views with you. Our hope is that our experience in this area can help some of you who may be struggling with these issues today.

Let's start by acknowledging that social networking in the workplace is highly controversial. Just google on "allow social networking at work," and you'll get thousands of pro, con and 'middle ground' articles.

In this paper we'll be looking briefly at these three positions. The basic question is, "To what extent, if any, should workers be permitted to engage in social networking 'on the job,' and why?"

## Pro (“In Favor of”)

The typical ‘pro’ answers are “worker morale” and “business benefits.”

**Worker Morale.** Workforce morale is obviously important, but in the context of social networking it leads us to another question, “Should employees’ morale be dependent on a personal activity that is not related to their work?” Put another way, “Shouldn’t their morale be more dependent on job satisfaction, relationships with management and co-workers, pay, benefits, workplace atmosphere, etc.?” At Wavecrest we find it difficult to argue against the latter.

**Business Benefits.** As mentioned earlier, there *can* be business benefits, particularly enhanced communications and collaboration among the business’ stakeholders, i.e., employees, associates, partner firms, customers, etc. Some analysts even predict that Web 2.0 sites and applications will someday replace email, instant messaging and collaboration programs such as Microsoft SharePoint. But reaching that point won’t be quick or easy. A McKinsey Survey states:

“Our findings suggest that after an initial period of promise and trial, companies are coming to understand the difficulty of realizing some of Web 2.0’s benefits. Only 21 percent of the respondents say they are satisfied overall with Web 2.0 tools, while 22 percent voice clear dissatisfaction. Further, some disappointed companies have stopped using certain technologies altogether.”

In the meantime, for those organizations that are moving towards Web 2.0, the question remains, “How do we maximize the benefits while minimizing the risks?” More specifically, the issue is, “How can we get our employees’ to restrict their use of social networking to business purposes only?”

## Con (“Totally Against”)

Several strong ‘risk’ arguments support the “con” position. Among these are: decreased productivity, network security breaches, bandwidth costs, network performance issues, legal liability, business information leaks, and damage to organizational reputation. These concerns are very real and very difficult to counter. Consider just one of these, i.e., decreased productivity:

“Nucleus Research, an IT research company, reported in July that employee productivity drops 1.5 percent in companies that allow full access to Facebook in the workplace. That survey of 237 corporate employees also showed that 77 percent of workers who have a Facebook account use it during work hours. It also found that some employees use the social networking site as much as two hours a day at work, and that one in 33 workers surveyed use Facebook only while at work. And of those using Facebook at work, 87 percent said they had no clear business reason for accessing the network.”

The other ‘con’ arguments are equally weighty. Issues related to security, bandwidth, litigation, proprietary data, and company reputation can be extremely costly.

## Middle Ground

This position lets workers engage in ‘personal’ social networking on a limited, monitored basis. With today’s sophisticated software and appliance solutions, the middle ground can be very flexible and selective, enabling management and IT to fine-tune and optimize their controls over all forms of Internet usage, including social networking.

So, given all these countervailing views, just how *does* an organization decide which position to take and how to implement it?

Here’s what our VP of Business Development, Dennis McCabe, has to say on the subject:

“First, let’s look at the overall picture. From a business perspective, Web 2.0 sites and applications, including those based on social networking, are a relatively new phenomenon. They show promise for enhancing the ability of organizations and their employees to communicate and collaborate with their internal and external associates, and they may even some day replace email, IM, forums, blogs and collaboration programs (like Microsoft SharePoint, etc.). But they have a considerable way to go before reaching that point.

With that in mind, let’s go back to the question of what is the ‘optimal approach.’ The question is far from simple. There is no “one size fits all” solution. And from a historical perspective, the issue is a recent one; consequently it has few guiding precedents. That makes the solution a complex judgment call.

And if the judgment is to be sound, it needs to be based on multiple factors, and the importance of each of those factors will vary from organization to organization. Among these considerations are: organizational culture,

managerial philosophy and style, workforce morale, the nature and objectives of the business, workforce demographics and skills, industry trends and statistics, competitors' approaches to the issue, network vulnerability, availability and cost of technological solutions, and the need for external communications.

Of these, perhaps the most fundamental issue is the last, i.e., the need for external business-related communications and collaboration. If the need is clear and extensive, then it might be beneficial to grant well-defined access to social networking sites to some – if not all – workers. On the other hand, if the need is small or non-existent, then it is probably best not to grant *any* kind of Internet access to the general workforce in the first place. Thirdly, if the need is 'in between,' the middle ground may be best.

Another key factor – one that we hear much about – is worker morale. While morale need not be the overriding consideration in devising a solution, it cannot be ignored. The good news is that skilled management can foster good morale no matter which solution they choose.”

Based on what we've learned at Wavecrest over the years, let's take a closer look at how this can be done.

As mentioned earlier, management needs to carefully analyze and weigh all the factors bearing on this subject. While doing so, they must ask themselves, “What's in the best *overall* interest of the business, taking into account the needs of the workforce, management, owners (e.g., stockholders) and customers?”

'Best interest' of course includes profitability. And profitability impacts the first three of these constituencies, including the workers. No profit, no business, no jobs. Consequently, the impact of social networking on the bottom line cannot be ignored.

Assuming that management has weighed all the factors, they now need to synthesize their findings and conclusions into a clear policy to govern the use of social networking as well as other Web sites.

The importance of 'policy' cannot be overemphasized. While it is not a total solution, it is certainly its foundation. All aspects of implementation and enforcement depend on the design and clarity of the policy.

A well-designed and thoughtful policy can go a long way toward controlling the use of social networking sites without damaging morale. To achieve this outcome though, management must clearly communicate the policy, including its underlying rationale, to the entire workforce. Once employees understand the risks (to themselves as well as the company) associated with at-work social networking, the vast majority will accept any restrictions in good spirit.

Unfortunately, human nature being what it is, some workers will still object to *any* restrictions— no matter how minimal or reasonable. Their predictable complaint is, “Restrictions such as monitoring and/or blocking indicate a lack of trust! We're all mature individuals, and management should trust us to do the right thing.”

But they miss the point. Trust is not the issue. As already mentioned, the well-being of the business is the issue. Skilled managers resolve 'well-being' issues such as 'social networking policy' the same way they do all other business-related issues. That is, they conduct 'risk vs. reward' and 'cost vs benefit' analyses to choose options that best serve the 'well being' of all the business' stakeholders.

So where does Wavecrest come down on this issue? Vice President Dennis McCabe concludes:

“As I mentioned earlier, there is no one “right” or “best” answer. Each organization has to develop its own solution. Hopefully they will base their approach on a thoughtful analysis of all the factors that we previously discussed.

In *general* though, at Wavecrest, we believe that a middle ground approach is *probably* best for most companies – *if it is well designed*. 'Well designed' means equipped with reliable security protections, a selectively applied filtering program and a comprehensive monitoring and reporting system.

Such an approach can support a flexible policy that allows for business use and a degree of carefully controlled personal use. And the monitoring component will enable management and IT to identify and correct a variety of Internet-related problems that are bound to occur under the best of policies and systems.”

We hope this helps a bit. If you would like additional information, feel free to contact us via email at [info@wavecrest.net](mailto:info@wavecrest.net), by phone toll-free (in US and Canada) at 1-877-442-9346 or visit our Web site at [www.wavecrest.net](http://www.wavecrest.net).