



Internet Monitoring: Options for Managing Internet Use

Wavecrest Computing
2006 Vernon Place
Melbourne, FL 32901
Toll-free: 877-442-9346
Voice: 321-953-5351
Fax: 321-953-5350

www.wavecrest.net

Web filters can be effective, but only when used as an adjunct to reporting — or better, when employed as part of an integrated, policy-based blocking/reporting approach.

Organizations lose an estimated \$50 billion a year in productivity due to employees Web surfing out of personal interest at the

Abstract

In today's world, most employees can easily visit Web sites from their workplace. This can be a boon for most organizations. That is, it gives their workers rapid access to useful applications and vast amounts of helpful information. However, that same access — *if not properly managed by people who understand human behavior and workplace management* — can result in king-size problems. The reason is simple. The extremely wide range of interesting content on the Web tempts many employees to waste extensive time surfing for personal reasons. Such all-too-human behavior can seriously degrade the potential benefits of personal computers and network resources in the workplace, and it can unnecessarily increase associated labor, legal and bandwidth costs.

This paper discusses this “people management” issue in some detail and outlines some alternative solutions. It first analyzes overall Web-use management approaches and policies, and then moves on to discuss three types of software-based Web-use management tools: (a) Web-access *filters* (also known as *blocking* solutions), (b) Web-use *reporting* programs and (c) *integrated filter/reporting* solutions.

After defining and describing these tools, the author discusses their advantages and disadvantages. (“Disadvantages” is probably not as good a word as “considerations.”) Of the three tools, Web-access filters are perhaps the best known. They're also somewhat controversial, particularly with respect to their effectiveness. For these reasons, the author focuses particularly closely on Web filters for the workplace.

The paper closes with three fundamental conclusions. First, Web filters *can* be effective, but only when used as an adjunct to reporting—or even better, when employed as part of an integrated, policy-based blocking/reporting approach. Secondly, to be most effective, the organization's overall Web-use management approach should be developed and implemented by individuals who understand human resource management. This typically means HR professionals and functional area managers. (Such individuals need only obtain *technical* support from IT specialists.) Finally, blocking and reporting tools must be selected with great care, and they should be obtained from firms that understand workforce management as well as Information Technology.

Part I - Introduction

It's no secret that employees' access Web sites via the Internet and intranets is increasing at a phenomenal rate. In most cases, these increases are tied to huge investments in network resources. Effective usage of these resources can be a boon to the organization, but misuse and abuse can be quite detrimental. Consequently, more than ever before, organizations need progressive, proactive, policy-based approaches to manage their workforces' online activities. Such approaches can help businesses and other organizations capitalize on the positive aspects of employees' Web access while controlling any related misuse or abuse. Web-use management approaches can be—and in many cases are—aided by IT applications that provide “Web-access blocking,” “Web-use reporting,” or both.

Blocking and reporting both have advantages and benefits. This is particularly true when used in conjunction with well-founded Internet usage policies. However, both approaches have disadvantages (perhaps a better term is “special considerations”). For several reasons, blocking is particularly controversial. This and other Web-use management issues are examined in some detail in this paper followed by an analysis of blocking-only, reporting-only and integrated blocking/reporting tools. However, before proceeding with these discussions and analyses, some background information may be helpful.

Part II - Background

The Internet Phenomenon. It's well known that use of the Internet and intranets by all types of organizations (business, education, government, military and others) is growing exponentially. Riding this wave, millions of workers and other members of these organizations use desktop computers or workstations in their daily jobs. These connections give them ready access to internal and external Web sites and e-mail capabilities. Such access is truly a "good news — bad news" phenomenon.

The Good News. From a business or mission-related perspective, workers, students and other computer users have many legitimate and positive reasons to access Internet and intranet Web sites. For example, they may need to make customer and supplier contacts, perform academic and scientific research, conduct vendor and supply searches, perform competitor analyses, analyze news, research government regulations and statutes, make business travel arrangements, track enterprise resource utilization, disseminate intra-corporate information, participate in inter-organizational collaborative projects, order materials and supplies, and track order status. These activities are becoming more and more integral to the performance of core enterprise functions every day. Such network usage can and does contribute much to the productivity, agility, efficiency and success of the enterprise.

The Bad News. On the other hand, Internet usage has significant *negative* potential. Because the Internet is so interesting, diverse, and information-rich, employees can—and often do—waste considerable working time and network resources accessing Web sites for personal reasons. Such casual surfing obviously lowers productivity and results in unnecessary cost. Additionally, it can imply an improperly utilized, poorly supervised, or poorly motivated work force. It can also be a sign of missed profit opportunities. Finally, casual surfing can lead to sexual harassment lawsuits against the employer if an employee's downloads—for example, pornographic images—are offensive to fellow workers.

Organizations lose an estimated \$50bn a year in productivity due to employees web-surfing out of personal interest at the workplace." — *Sacramento Bee*

"Employees spend 90 minutes daily surfing the Internet at work for their own interest." — *Webster Network Strategies*

Part III — Web-use Management: Overcoming "the Bad" and Ensuring "the Good"

Because of the importance and cost of Internet (and intranet) usage, it is critically important for businesses and other enterprises to carefully manage the way in which these vital resources are used. In our judgment, the objective of such management should be to capitalize on the beneficial, productive potential of network resources while precluding or minimizing their negative potential. An important corollary is to do this in a balanced way, one that promotes the interest of the enterprise as a whole without creating a resentful and/or oppressive climate in the work place. This is a delicate balancing act, one that is somewhat difficult to define and achieve. The challenge stems from the fact that behavior that is considered "abuse" in one enterprise may be perfectly acceptable, even desirable, in another. ("One man's meat is another man's poison.") But then, objectives that are worthwhile are never easy to achieve, and the obstacles can be overcome. It's worth it. Read on.

Note: Our concern for waste and abuse does not imply a need to "spy" on the work force or violate their right to privacy. Such concern is a legitimate management issue. In a broad sense, it's no different from concerns found in all enterprises relative to misuse and abuse of other enterprise resources. Examples include concerns involving telephone privileges (for personal calls), wasted electricity, theft of company property, use of company vehicles for personal use, etc. Like network abuse, all of these forms of negative behavior detract from the organization's efficiency and productivity and increase operating costs.

General Web-use Management Approaches. Until recently, the majority of Web-use management efforts have been aimed *solely* at preventing or minimizing use of the Net for

It is critically important for organizations to carefully manage the way in which vital network resources are being used. The approach must be balanced, minimizing Web abuse while promoting business-related Web activity.

The effectiveness of the blocking process depends on the quality of the list. Most blocking-only software programs use lists with a limited number of categories focusing on legal liability risks.

personal reasons. Some organizations do this by automatically blocking access to “undesirable” sites, e.g., those featuring pornography. At the same time, others do it by using reporting techniques that automatically identify users (“visitors”), list the sites they have visited, and provide reports to management for assessment and action if required. And yet others do both. For the most part, to date, the focus of all of these techniques has been on the negative side of the issue, i.e., overcoming “The Bad.”

More recently, the trend is tilting a little more toward ensuring “The Good,” and toward viewing Web-use management more positively, i.e., as a way to improve productivity and profitability without damaging morale.

The concepts and approaches summarized above may or may not be policy-based. That is, they may or may not be used in close conjunction with written computer usage policies. Visit www.wavecrest.net to see related white papers on policy-based Net-use management concepts and approaches.

With this background in mind, we now come to the main purpose of this paper — comparing the various Web-use management approaches and tools to each other.

Part IV —Specific Approaches and Techniques

General. Fundamentally, there are three approaches to Web-use management: (a) Web-site or Web-access blocking, (b) Web-use reporting, and (c) integrated Web-use management, i.e., blocking plus reporting. Let’s look briefly at all three and examine their relationship to Web-use policies and corporate cultures.

Web-site Blocking. In the workplace (as opposed to household situations), Web-site blocking (aka filtering) is a computerized process that automatically prevents the organization’s computer users from visiting certain Web sites. These “prohibited” sites — or categories of sites — are those that management considers inappropriate or unacceptable. Naturally, the definition of “inappropriate” and “unacceptable” will vary from organization to organization. However, *typical* examples of inappropriate or unacceptable sites are those that can be categorized as pornography, shopping, travel, chat, etc. In any case, most blocking processes can accommodate organizational variations.

Blocking processes typically rely on software that functions in real time. First, the software compares the URL in a user’s “visit request” with the URLs in a built-in, pre-developed control list of Web sites that *might* be visited. (The sites in the list are grouped in categories that have been pre-designated by management as inappropriate or unacceptable.) If the software finds a match between the requested URL and a URL that’s in a prohibited category, the visit request is denied, and (usually) the user is so notified. On the other hand, if no match is found, the request is granted.

Obviously, the effectiveness of the blocking process depends on the quality of the control list. That is, for the process to be effective, the list must contain all — or at least most — of the inappropriate or unacceptable sites that might be visited, and they must be properly categorized. Because the Web is so vast and fast growing, no list is perfect with respect to these issues. However, some are better than others, depending on how they are constructed and maintained. (Note: most blocking-only software programs use lists with a limited number of categories that focus almost exclusively on “totally unacceptable” sites that carry legal liability risks.)

Did You Know:

30-40% of Internet use in the workplace is not related to business.

— *IDC Research*

70% of all Internet porno traffic occurs during the nine-to-five workday.

— *Sex Tracker*

37% of workers say they surf the Web constantly at work.

— *vault.com*

Web-use Reporting. Web-use reporting is another software-based Web-use management process. Rather than filtering, its overall purpose is to monitor and report on how a workforce or other networked group of users (such as soldiers or students) uses its access to Web

Well-designed, integrated approaches combine both blocking and reporting capabilities, and they utilize a broad-based categorization list.

sites. More specifically, reporting programs keep management informed as to which users visited which sites, when they did so, how often they did so, and the type of content they were seeking. Well-designed software products can focus and report selectively on the activity of individual users, specific workgroups (departments) or entire enterprises. Well-designed products also automatically highlight cases of abuse based on the organization's own Web-use policy (assuming they have one). In any case, regardless of design, managers typically assess the information in the reports to determine the appropriateness of the workforce's network resource usage. They then use their conclusions to adjust workplace processes, modify blocking practices (if used) and take specific personnel actions.

From a technical perspective, most reporting programs use URL categorization lists that are *conceptually* similar to those discussed earlier under blocking software. However, lists in the better reporting programs are more comprehensive than those in most blocking programs. A more comprehensive list, with its broader scope of categories, results in reports that are much more complete and accurate than those produced by programs that use a narrow-scope list that was originally designed for blocking only.

“Companies that do not monitor employees' surfing habits make themselves vulnerable to legal liabilities, probable bandwidth abuse and employee productivity gaps.” — *The Aberdeen Group*

Integrated Blocking/Reporting Approaches. Well-designed *integrated* approaches combine both blocking and reporting capabilities, and they utilize a broad-based categorization list. As implied in the discussion above, a broad-based list assumes that *all* Web site categories are important, not just those that put the organization at risk of legal liability.

Relationship to Web-use Policies. Our research and our management experience indicate that the best Web-use management approaches — whether blocking, reporting or integrated — are *policy-based*. Effective policy-based approaches have three desirable characteristics.

1. The Web-use management approach (do's, don'ts, monitoring methods, blocking methods, etc.) is described in detail in a clearly written Internet usage policy, often referred to as an Acceptable Use Policy (AUP).
2. Workers are trained on proper use of network resources and briefed on the provisions of the AUP.
3. HR personnel are intimately involved in the development and administration of the approach.

Cultural Considerations. Our research also indicates that corporate culture has a great deal to do with Web-use management. As common sense would tell you, *variations* in culture have produced a wide spectrum of beliefs and approaches concerning the subject. A few organizations feel that Web-use management is totally unnecessary. Others believe that all they need to do is simply to publish a policy that urges employees not to spend *excessive* time surfing the Web for personal reasons. Still others feel that spot-check reports are all that's needed — with management taking action only in extreme cases of abuse. Others believe that continuous use of highly comprehensive summary-level reports and detailed audits are mandatory; managers in such organizations feel that such reports and audits enable them to simultaneously optimize employees' use of Web-access resources, improve workforce productivity and avoid legal liability. Still other organizations believe that a Web filter alone will preclude any problems. And yet others believe that a total, integrated policy-based approach incorporating both reporting and filtering are absolutely necessary to maximize productivity and minimize costs related to the use of network resources. Because of this multitude of cultural variations, Web-use management tools must be well-designed so that they can be easily configured to conform to any of them.

Privacy, Morale and Legal Considerations. Closely related to cultural considerations are the issues of privacy, morale and legality. Do employees have *any* right to privacy in the workplace, and if so, how much? The question is openly debated at times, has never been completely settled, and has obvious implications for workforce morale. On the other hand, for the most part, courts have upheld the rights of employers to monitor and/or block employee's access to Web sites in the workplace — especially if the employees have been notified in

For the most part, courts have upheld the rights of employers to monitor and/or block employee's access to Web sites in the workplace, especially if the employees have been notified in advance that this is being done.

In today's complex world, filtering should only be one part of an effective Web-use management approach.

advance that this is being done. Another legal issue that relates to employee Web-use management is sexual harassment. As mentioned earlier, casual surfing can lead to sexual harassment lawsuits against the employer if an employee's downloads—for example, pornographic images—are offensive to fellow workers. The bottom line? It behooves organizations to carefully consider *all* of these issues when choosing a Web-use management approach.

And what does the author think? He believes the following. Although privacy, morale and legality issues are a bit complex and sensitive, competent managers — with a bit of effort — can find the right balance between employees' rights and morale on the one hand and management's need to maximize productivity and avoid legal liabilities on the other. However, the right balance cannot be simplistic. It should use all the resources at management's disposal: sound usage policies, clear communications with the workforce, and well-designed tools. And finding that right balance involves, among other things, knowing the advantages and drawbacks of the available tools, as discussed next.

Part V — Advantages and Drawbacks of Blocking and Reporting Tools

General. Web-access blocking and Web-use reporting tools both have a number of advantages, and they both have a few “disadvantages.” In the author's view, the latter are not true disadvantages or actual shortcomings; they are simply factors to consider in developing an overall Web-use management approach. Let's take a look.

1. Blocking Tools

Web filters (blocking software) prevent users from accessing management-specified Web sites or categories of sites. The advantages and drawbacks to using a filter-only approach are outlined below.

A. Advantages.

Blocking (also known as filtering) provides a measure of protection from legal liability. It does this by preventing employees from visiting sites that portray or discuss inappropriate subjects such as pornography, gambling, hatred, terrorism, “bomb-making”, illicit drugs, etc. Such visits could possibly be connected to illegal acts for which the enterprise might be held liable.

1. To a significant extent, blocking can preclude situations in which workers can be offended, feel sexually harassed, or become upset because they saw pornography on another user's computer screen. Such incidents could result in sexual harassment suits.
2. If the organization *does* find itself being sued for situations such as those described in bullets 1 and 2, the courts are more likely to rule in its favor if a good-faith blocking process is in place, even if that process failed in the case under consideration.
3. Blocking can help minimize wasted time caused by casual surfing.
4. After it is set up, blocking works automatically, and it requires very little administration.

B. Drawbacks and Other Considerations.

1. A blocking-only solution tends to ignore the large amounts of employee time wasted on inappropriate sites that are not included in the blocked categories. In addition, it doesn't let management know how many and which unacceptable visits are going undetected.
2. Members of the workforce may view the practice as too intrusive, intimidating and autocratic. In addition, blocking can trigger time-consuming and disruptive debates about First Amendment issues, right to privacy, etc.
3. Filtering may prevent workers from doing a good job. This can happen due to work-related sites being mistakenly blocked.
4. Because the Web is so vast and fast growing, some truly unacceptable sites may not be included in the filter's control list and thus not be blocked.

A blocking-only solution tends to ignore the large amounts of employee time wasted on inappropriate sites that are not included in the blocked categories.

5. Without a reporting capability, filtering provides no categorized site-visit data; such data could be very useful for managerial decision-making and strategy-setting purposes in mission-critical areas.
6. Filtering by itself is not a “positive” approach; i.e., it doesn’t encourage or foster use of network resources for work-related or mission-critical functions. And it does not help management or employees use the Internet for positive, constructive purposes.
7. Filtering by itself provides no resource-consumption data to aid managerial decision-making with regard to IT hardware/software requirements.

C. Summary. Weighing the advantages and disadvantages of filtering, we can say the following. In today’s complex E-world, filtering should only be a *part* of an effective Web-use management approach. A truly effective Web-use management approach involves much more. In addition to a filtering component, such an approach includes:

- Establishment (by senior management) of a broad, comprehensive Web-use policy.
- Policy provisions that guide productive use of network resources while facilitating the detection and prevention of abuse.
- Establishment of clear guidelines for policy administration.
- Detailed orientation of users.
- Policy-based reporting (discussed below).
- Management follow-through.

2. Web-use Reporting Tools

Web-use reporting can be very simplistic and basic, or it can be quite comprehensive and advanced. In general, a basic reporting program simply lists the URLs visited by a user or group of users. This leaves it up to the recipient of the report to analyze and evaluate the activity — a daunting task at times. On the other hand, typically, a more comprehensive reporting tool can be set up to automatically analyze the activity in terms of acceptability relative to the organization’s usage policy. It can also highlight abuse — as defined by management in terms of visit-thresholds. (A threshold is a specified number of allowable visits in a 24-hour period.) Let’s examine the advantages and drawbacks of each type of reporting.

A. Basic Reporting Products. Basic reporting products have a few advantages and several disadvantages, as listed below.

a. Advantages. While somewhat limited, basic reporting products do have a few advantages. They can:

- Provide reasonable visibility into total usage (numbers of hits).
- Provide reasonable visibility into resource consumption (megabytes used).

b. Disadvantages. Unfortunately, these products are somewhat limited, i.e., they:

- Require extensive manual analysis and interpretation to determine “appropriateness” of visits (acceptable, unacceptable, etc.).
- Don’t come with clear, uniform standards for use in the interpretation effort.
- Are subject to possible misinterpretation of results (false accusations, etc.).
- Are not an effective educational tool for Web-use.
- Offer slightly less protection from legal liability (compared to blocking).
- Provide reports that contain only “raw *data*,” not usable *information*.

A basic reporting program simply lists the URLs visited by a user or group of users. A comprehensive reporting tool can automatically analyze activity as acceptable or unacceptable according to your guidelines or specific Internet usage policies.

A well-designed, policy-based reporting tool is highly flexible and customizable. This feature facilitates future adjustments in policy within the enterprise.

Comprehensive, policy-based reporting works well with both very rudimentary and very sophisticated policies; is comprehensive, customizable and flexible; and offers excellent protection against legal liability.

c. Summary. Simple, basic reporting that is not policy-based is cheap and it can be useful, but only in a very limited way. It also requires considerably more managerial and administrative effort than other methods.

B. Advanced, Policy-Based Reporting Products

a. Advantages. A well-designed policy-based reporting tool has a number of significant advantages. Such a tool...

- Enables reporting processes and formats to correspond to, be driven by, and use the same terminology as the usage policy provisions.
- Ensures that analyses and interpretations of results are based on clear, uniform standards (built into the policy). This helps ensure consistent, fair administration.
- Is highly flexible and tailorable. This feature accommodates policy variations from one enterprise to another. It also facilitates future adjustments in policy within any one enterprise.
- Offers good visibility into categorized site-visit activity — by department or by individual user. This helps pinpoint productive and nonproductive use.
- Provides good visibility into network resource consumption (megabytes used). This helps management know if and when additional network capacity is needed.
- Serves as a good “educational” tool, ensures work force understanding, and lends itself to worker or student orientation. This leads to better acceptance of the policy and associated auditing processes.
- Can be used to guide and encourage *constructive* use of network resources as well as to curb abuse. This leads to increased productivity and enterprise success.
- Facilitates *controlled* use of network resources for personal reasons. This enhances morale and thus productivity.
- Does not interfere with workers making legitimate site visits. This maximizes productive use of resources.
- Can be used in conjunction with filtering. This capability gives the enterprise more choices as to how to manage their resources.
- Provides automated analysis and interpretation of results (e.g., acceptable, unacceptable, etc.) Through standardization, this feature prevents almost any possibility of misinterpretation of results (false accusations, etc.). It also minimizes the amount of management time required.

b. Special Considerations. There are no actual disadvantages associated with policy-based reporting. However, there are some factors that need to be taken into account when considering its use. That is, policy-based reporting:

- Works best when the enterprise employs a comprehensive Web-use policy, one with highly specific provisions governing usage. (All enterprises really need such policies regardless of - and independent of - software considerations.) Such provisions can be translated directly into software settings to automatically determine “acceptability,” “abuse,” etc.
- Works best when enterprise IT and vendor personnel collaborate to optimize startup and administration of the overall policy-based approach. (The right vendor can provide policy templates, sample policies, and general advice and assistance with startup and administration.)
- Is somewhat more sophisticated than blocking and/or simple reporting, and may require a little more training.
- Is a little more expensive than *simple* reporting (but offers much more).
- Requires commitment and initial involvement by management.

d. Summary. Comprehensive, policy-based reporting has numerous advantages and no disadvantages. It works well with very rudimentary or very sophisticated policies, and it can help support the organization’s prime mission objectives while helping to curb abuse. It is comprehensive, flexible and tailorable and, in the author’s view, offers excellent protection against legal liability.

3. Integrated, Policy-Based Blocking and Reporting

For many if not most organizations, an overall approach that integrates Internet usage policy with Web-access filtering and Web-use reporting will offer the best solution. Such an approach recognizes that Web-use management is a relatively complex *people* issue, not simply an IT-security or computer technology problem. And like most people issues, it doesn’t lend itself to simplistic one-dimensional solutions, particularly when none of them are perfect. With an integrated solution, managers can set up policies to guide employees’ as well as their own actions, examine reliable reports to help them gauge conformance to policy, and institute filtering processes to help prevent a major portion of the problem.

A. Advantages. Simultaneous policy-based use of both approaches provides numerous advantages. In fact, it will provide all of the advantages cited above for blocking and *advanced* reporting. See 1.A and 2.B.a (above) for details.

B. Disadvantages. Because it significantly mitigates the drawbacks of a blocking-only approach, an integrated, policy-based blocking and reporting entails almost no real disadvantages. The few considerations that are in play are similar to those discussed above under advanced policy-based *reporting* (see 2.B.b above).

C. Summary. An integrated, policy-based approach obviously offers the most coverage and protection, albeit at slightly higher cost than a blocking-only or reporting-only approach.

With an integrated solution, managers can set up Internet usage policies, examine reliable reports to help them gauge conformance to policy, and institute filtering processes to help prevent much of the problem.

Web use management is a people issue, not merely an IT or IT security problem. HR and business unit managers must obtain technical assistance from IT, but they should take the lead in developing Web-use policy and management processes.

Part VI. Conclusions and Recommendations

Conclusions. In general, three resources are available to help progressive organizations manage their employees' use of Web-access resources: (a) Internet usage policies, (b) Web-use *reporting* software, and (c) Web-access *filtering* software. Depending on the organization's size, culture and workforce characteristics, management should use at least one of these to help curtail casual surfing and optimize employees' use of network resources. However, in most cases, it's best to combine all three into an integrated approach. That's because filtering alone is somewhat limited and reporting alone, while quite effective, doesn't have real-time control capability. On the other hand, the policy-based integrated approach provides maximum deterrent effect, control capability and managerial visibility. These capabilities work together to help managers and administrators increase productivity and reduce labor, legal and bandwidth costs.

Recommendations. Underlying all other recommendations is a principle that is absolutely fundamental, i.e., *Web-use management is a people issue, not an IT or IT-security problem.* With this recognition in mind, businesses and other organizations should assign a team of people that understand human resource management to design and implement an integrated Web-use management approach. This typically means HR personnel and business unit or line organization managers. Such individuals can obtain *technical* assistance from IT, but they should *take the lead* in developing Web-use policy and management processes. They should also take the lead in establishing requirements for a cost-effective software tool(s) to support the overall effort. Among those requirements should be assurance that the tools have been designed from the ground up for use with an integrated approach. Finally, the team needs to ensure that such tools are obtained from a firm that understands workplace management as well as it understands information technology.