Mark Rizzo, vice president of operations and platform engineering at Perpetual Entertainment Inc. in San Francisco, learned in a previous job the consequences of not protecting intellectual property. "I have been on the side of things disappearing and showing up at competitors," he says. The start-up online game developer deployed Tablus's Content Alarm to remedy the problem. Rizzo uses it to look for suspicious activity, such as large files that are moving outside the corporate LAN. Now that the basic policies and rules have been set, the system doesn't require much ongoing maintenance, he says. Still, Rizzo doesn't use blocking because he would need to spend significant amounts of time to create more policies in order to avoid false positives.

Although companies in highly regulated industries can justify investing in outbound content monitoring and blocking tools, other organizations may have to sharpen their pencils to justify the cost. These are very expensive solutions to deploy. Fredriksen, who built a system to support 16,000 users, says that for a setup with about 20,000 users, "you're in the $200,000 range, easily."

With outbound content management tools, "you can build very sophisticated concept filters," says Cliff Shnier, vice president for the financial advisory and litigation practice at Aon Consulting. Typically, the tools come with templates for types of data that most enterprises want to filter, and they can analyze contents of servers and databases to derive filters for company-specific information, he says. (Consulting firms can improve these filters using linguists and subject matter experts.)

As any user of an antispam tool knows, no filter is perfect. "A big mistake is to have too much faith in the tools. They can't replace trust and education," says consultant Kocher. They also won't stop a determined thief, he says.

Even when appropriately deployed, these tools don't create an ironclad perimeter around the enterprise. For example, they can't detect information that flows through Skype voice over IP (VoIP) service or SSL (Secure Sockets Layer) connections, Kocher notes. They can also flood logs with false positives, which makes it hard for IT security staff to identify real problems.

That's why chief information officers should look at outbound content management as a supplemental tool to limit accidental or unknowing communication of sensitive data, not as the primary defense. Fredriksen says that although Vontu is important, it's still just one piece of a larger strategy that includes an overlapping set of controls that Raymond James uses to combat insider threats. "This augments the intrusion–detection and firewall systems we have that control and block specific ports," he says. "It's just a piece. It's not the Holy Grail."

Source: Adapted from Galen Gruman, "Boost Security with Outbound Content Management," *CIO Magazine*, April 9, 2007; and Robert Mitchell, "Border Patrol: Content Monitoring Systems Inspect Outbound Communications," *Computerworld*, March 6, 2006.

CASE STUDY QUESTIONS

1. Barring illegal activities, why do you think that employees in the organizations featured in the case do not realize themselves the dangers of loosely managing proprietary and sensitive information? Would you have thought of these issues?
2. How should organizations strike the right balance between monitoring and invading their employees' privacy, even if it would be legal for them to do so? Why is it important that companies achieve this balance? What would be the consequences of being too biased to one side?
3. The IT executives in the case all note that outbound monitoring and management technologies are only part of an overall strategy, and not their primary defense. What should be the other components of this strategy? How much weight would you give to human and technological factors? Why?

REAL WORLD ACTIVITIES

1. Technologies such as VoIP used by Skype and similar products make it more difficult to monitor outgoing information. Search the Internet to help you understand these technologies and why these problems arise. Other than banning them, what alternatives would you suggest to companies facing this problem? Prepare a presentation to deliver your recommendations.
2. As a customer of many of the companies noted in the case, or others in the same industries, what is your expectation about the measures and safeguards that these organizations have implemented to protect inappropriate leaking of your personal information? After reading the case, has your expectation changed? Break into small groups with your classmates to discuss these issues.