Information Technology

Technological developments continue to yield greater sales, improved customer relations and increased collaboration with vendors and suppliers. Yet, privacy issues and intellectual property concerns may create roadblocks for IT companies seeking to take advantage of these trends. What key issues should corporate counsel watch in order to keep their companies in a leadership position?

KEEP IT CLEAN: HOW TO MANAGE THIRD-PARTY TECHNOLOGY

In addition to intellectual property considerations, savvy corporate counsel will take a number of steps to protect their company's technology developments. Policies and procedures should be put into place to handle incoming technology, in particular a supplier's trade secrets that could prevent the company from independent development or use of related know-how. "Clean rooms" and other safeguards should separate the individual recipients of supplier technology from in-house developers. Confidentiality agreements with suppliers also should be carefully drafted to ensure that they do not unduly restrict the organization's technological growth.

Likewise, corporate counsel should ensure that the company is aware of the implications of the use of open source software by its developers and in any software acquired from suppliers. Open source software license terms frequently require the open source code and any works with which it is combined be licensed at no charge, severely limiting the potential for commercialization. Representations and warranties should be obtained from in-house developers and external suppliers as to the extent of open source content of their code.

Corporate counsel also should recognize that a license grant, which does not expressly permit assignment or sublicensing, may not in fact be assignable or sublicensable. Silence as to assignability or sublicensing may not mean that they are permitted. Prudent counsel will ensure that all licenses expressly deal with the issues of assignment and sublicensing, as well as make certain that other provisions, such as license restrictions, scope of rights and confidentiality covenants, do not conflict with the assignment and sublicensing terms.

Lisa K. Abe
Partner, Information Technology Group
Blake, Cassels & Graydon LLP
lisa.abe@blakes.com

CONTROLLING ACCESS AND USE: MANAGING DIGITAL RIGHTS

As companies collaborate with vendors or suppliers or outsource design and programming work, counsel should pay close attention not only to how products are used and developed, but product distribution as well. This is particularly important with digital goods, such as software, music and other media. In addition to the issue of lost revenues, leaked pre-release software may be unstable or corrupt files on a user's computer, tarnishing a company's image with customers unaware the product in question is not a final build.

Implementation of a digital rights management (DRM) solution can alleviate many of these issues. DRM programs control access to and the use of a work, not its sale. Many options are available, each providing different controls. Some regulate end use, others restrict access and yet others prevent copying or modification by unauthorized persons. Selecting the proper DRM implementation also may enhance synergy with third parties.

Further, corporate counsel should be aware of intellectual property issues when a third party is hired to produce part or all of a product. Failure to treat information as confidential or restrict access thereto may waive legal protection. Similarly, any development agreements should clearly set forth who owns any intellectual property resulting from a development effort. The inclusion of a "work for hire" clause is useful in maintaining copyrights in any software or code developed by outside entities. Likewise, a clause in any development agreement assigning all patent and trade secret rights to counsel's company may prevent disputes that could otherwise stall design efforts.

S. Craig Hemenway
Associate, Patent Practice
Dorsey & Whitney LLP
hemenway.craig@dorsey.com

GIVING CUSTOMERS THE COMPLETE PICTURE

Corporate counsel must be aware of how their companies' IT products and claims are positioned. As customers seek single-source solutions to IT privacy, security, data integrity and data management, IT companies may find it all too easy to claim their products deliver these solutions. Yet electronic data can be accessed, duplicated and used in multiple ways, or altered or deleted, whether accidentally or maliciously. Companies claiming to address every concern leave themselves open to criticism, loss of market share and potential liability for misrepresentation.

For example, email filtering software only fends off viruses in email; separate solutions address instant messaging viruses. The Federal CAN-SPAM Act prohibits certain unsolicited commercial email, and multiple technological approaches are needed to ensure that no employee can send email to prohibited addresses. Also consider California's new Web site privacy policy law, which took effect July 1, 2004. Companies gathering certain information from California residents must post policies describing categories of information collected and third parties with whom it may be shared. Software products track Web site actions and create warnings when the privacy policy needs amendment. However, the software company must make clear that customers are also separately responsible for tracking and disclosing any sharing of data after it is transferred to multiple PCs, handheld devices and disparate software programs. Counsel can play a critical role in ensuring that their companies do not provide half-solutions or misrepresentations to customers.

Ethna Piazza
Partner, Corporate and Intellectual Property
Sheppard, Mullin, Richter & Hampton LLP
epiazza@sheppardmullin.com

MANAGING SECURITY IN GLOBAL OUTSOURCING

Companies moving to global outsourcing should focus on four critical security issues as they structure their relationships. First, counsel should ensure that the company undertakes proper due diligence of prospective vendors. A detailed questionnaire should be presented about such issues as financial condition, information security practices and disaster recovery. Has each vendor had security audits and do they comply with/been certified by the appropriate standards organizations? Even the largest technology vendors may not use the security measures mandated of a health care or financial organization. The questionnaire and vendor answers should be included in the outsourcing agreement.

Second, counsel should require background checks on the vendor personnel who will be involved in each project. These employees will handle the company's most sensitive information and relationships—software development, trade secrets and business process design. Counsel must ensure adequate steps are taken to protect the company's data and customers as well as weigh the cost of due diligence against the importance of the data and liability exposure for failing to provide protection.

Third, companies must comply with the wide variation of data protection laws around the world. To effectively address the relationship's compliance, counsel need to analyze the data flows—what information is going between the company and the vendor—and determine the joint strategy for compliance.

Finally, focus on the contract protections themselves, making certain all of these details are spelled out. By underscoring the importance of security as outlined above, counsel will be surprised at how easily they can affect standard vendor positions and enhance their company's baseline security protection.

James R. "Jim" Kalyvas
Partner, E-Business & Information Technology
jkalyvas@foley.com

Michael R. Overly
Partner, E-Business & Information Technology
moverly@foley.com
Foley & Lardner LLP

To prepare their companies for the wide range of regulatory requirements expected to unfold, counsel should design outsourcing contracts defensively, as well as set clear security parameters for data handling.

DO PRIVACY RISKS DOOM OUTSOURCING?

Privacy concerns threaten to stall outsourcing. The U.S. Congress earlier this year blocked federal agencies from doing it. The Federal Deposit Insurance Corporation issued guidance for banks, in June, on how to handle outsourced data. In both Canada and Europe, unions, aiming to save local jobs, have challenged regulators to examine whether privacy is compromised when data crosses borders.

In fact, the best offshore outsourcing companies are heeding these concerns and are building protections that exceed North American norms.

To prepare their companies for the wide range of regulatory requirements expected to unfold, counsel should design outsourcing contracts defensively, as well as set clear security parameters for data handling.

Contracts should include detailed service level agreements specifying who can see what data, what can be done with it and how data can be combined, if at all. Subcontracting should be prohibited. The vendor must accept external compliance audits and regulatory inspection. In fact, North American regulators now insist that they be allowed to inspect data being handled offshore.

Security standards should meet ISO 17799 and BS7799 norms, international standards for information security management, monitoring security and assessing risks. Counsel should make certain that they have a back-up server outside the outsourcer's country and should feel confident about disaster recovery plans. Outsourcing agreements also should contain requirements for record management and audit trails, as well as stipulations for encryption of sensitive data.

Taking active steps now will make it clear to customers and regulators that your business has made every reasonable effort to ensure that sensitive data is protected.

Simon Chester
Partner, KNOW*law*™ *Group*
McMillan Binch LLP
simon.chester@mcmillanbinch.com

A NEW, NARROWER WILLFULNESS DOCTRINE?

Since early February, technology and patent attorneys have been waiting for the opinion of the U.S. Court of Appeals for the Federal Circuit in *Knorr-Bremse Systeme Fuer Nutzfahrzeuge GmbH v. Dana Corp*. In September 2003, the Court asked these parties, in a *sua sponte* grant of rehearing *en banc*, to argue whether the inference in willful patent infringement cases should be changed.

The Federal Circuit requested briefing on four questions:

1. When the attorney-client privilege and/or work product privilege is invoked by a defendant in an infringement suit, is it appropriate for the trier of fact to draw an adverse inference with respect to willful infringement?
2. When the defendant has not obtained legal advice, is it appropriate to draw an adverse inference with respect to willful infringement?
3. If the court concludes that the law should be changed, and the adverse inference withdrawn as applied to this case, what are the consequences for this case?
4. Should the existence of a substantial defense to infringement be sufficient to defeat liability for willful infringement even if no legal advice has been secured?

Thirty *amici* briefs were filed; 29 of them favored elimination of the adverse inference. The Federal Trade Commission also has proposed a narrower willfulness doctrine.

While it remains unclear how far the Court will go in abrogating existing adverse inferences, the opinion will likely result in a new set of standards. Prudent counsel will read the opinion closely, then formulate and implement new practices that reflect those standards.

Peter E. Strand
Partner, Litigation
Shook, Hardy & Bacon L.L.P.
pstrand@shb.com

For more information about these lawyers and their firms, please visit www.martindale.com.