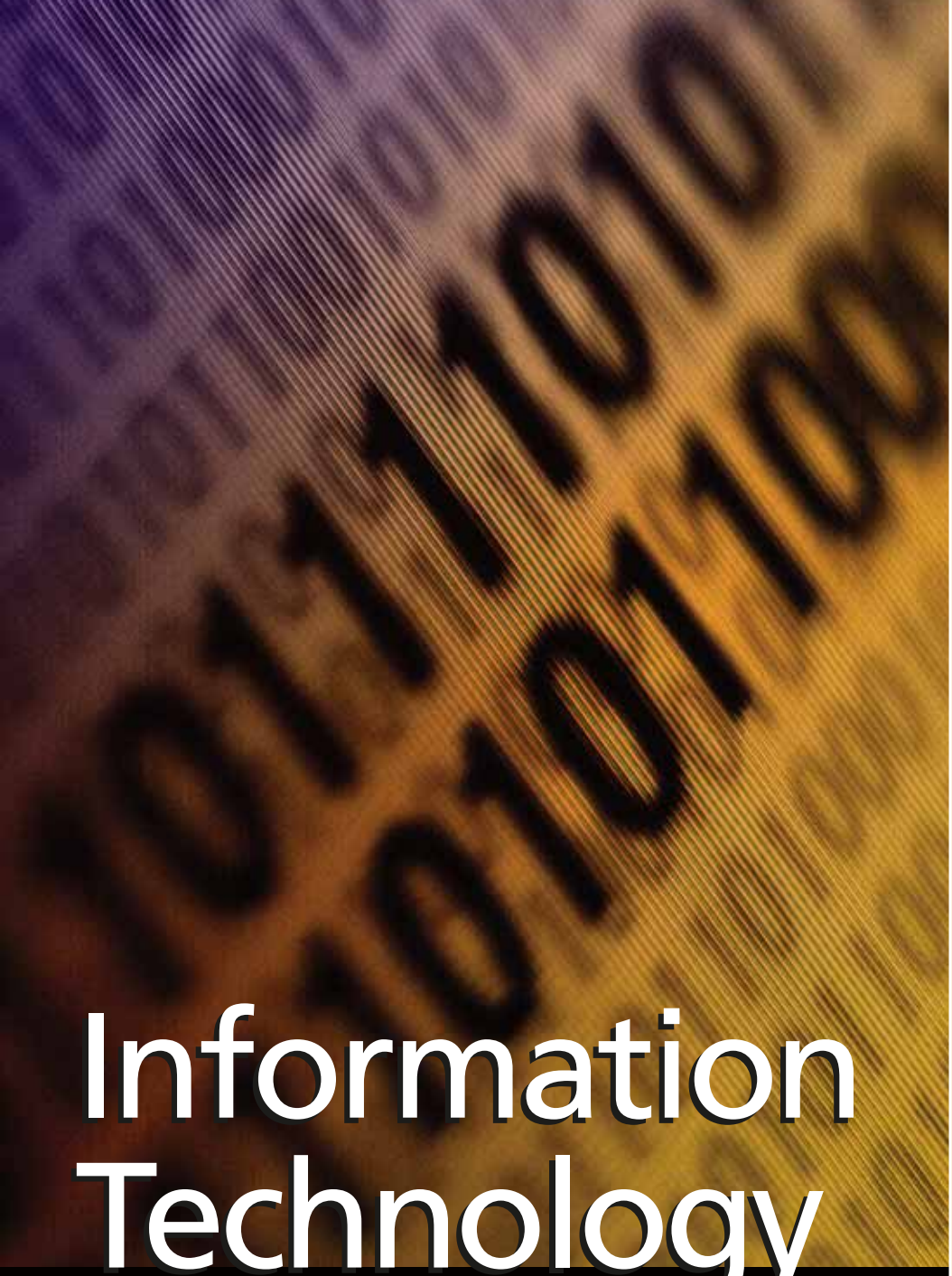

Information Technology

Information technology is at the far horizon of evolving law. Intellectual property issues dominate, from copyright infringement to proactive patent strategies. IT vendors also face the impact of new e-discovery rules. Add the need for proactive counsel on software licensing and contractor security, and in-house IT counsel face major challenges to keep ahead of the curve.

Steve Cole/Photodisc Green/Getty Images

INTELLECTUAL PROPERTY INDEMNITIES

Software product vendors typically provide intellectual property indemnification in software licensing agreements, including stand-alone licensing agreements, Original Equipment Manufacturer (OEM) agreements (where the software is to be bundled with other software or provided with computer hardware) and value-added reseller agreements (where the vendor has modified the original software). Indemnities assure end users that the vendor is selling legitimate title to the software, and that the users will have protection in the event they are sued for infringement by a third party demanding anything from surrender of the software to imposition of monetary damages. Most indemnity clauses use standard language, but vendors and purchasers may wish to modify indemnity terms to their own advantage.

Counsel for software vendors, for example, can seek to limit vendor liability in an infringement lawsuit to the end user's original purchase price or annual license fee, thus capping any potential damage awards. Vendors may also reserve the right to specify and hire infringement defense counsel, as well as the right to approve any final settlement. End users' counsel, by contrast, can seek vendor indemnity against any and all infringement allegations involving the software's patents, copyrights, trademarks and business methods. Users may also want to define protection for derivative works developed using the software. Either side may seek to specify geographic coverage—vendors to U.S. patent law only, end users to potential intellectual property rights violations arising globally.

Software vendors formerly were reluctant to modify indemnity terms. However, highly competitive conditions in the technology marketplace can give end users greater leverage to negotiate coverage. As in all deals, attention to contract language can lead to more effective negotiations. Both vendors and end users should be fully aware of future risks.

Mark Naftel
Of Counsel, Business and Technology
mnaftel@bakerdonelson.com

Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

PROACTIVELY MANAGING SOFTWARE SOURCING

Because software sourcing decisions cannot readily be undone, all companies should implement policies that review the acquisition and application of open source software before acquisition decisions are made. The decision to choose software is typically a technical one, but it should be subject to full legal and management assessment in a formal purchasing and/or product development process. Such a process can educate both developers and users about the implications of software licensing agreements before they commit to using open source software products.

Developers using open source software and licensees of open source products can easily run afoul of the license terms—causing problems that catch management unaware. By contrast, thorough investigation can identify legal and business concerns that are raised by many open source license agreements, such as proprietary code disclosure requirements. Proactive business and legal review can also identify potential product warranty and intellectual property infringement deficiencies that are prevalent in most open source license agreements.

Management should be cognizant that the use of open source software may still (despite its increasingly widespread use and adoption) raise issues in some corporate/commercial transactions, particularly in the purchase/sale of technology-based companies where a large portion of the sale price is to be derived from underlying (and supposed proprietary) intellectual property. Substantial use of open source software may create significant due diligence and valuation issues and concerns for each of the seller and purchaser.

Robert L. Percival
Partner, National Co-Chair, Technology Law Team
rpercival@ogilvyrenault.com

Marc A. Tremblay
Partner, National Co-Chair, Technology Law Team
matremblay@ogilvyrenault.com
Peer Review Rated

Ogilvy Renault LLP

IT CONTRACTOR SECURITY

As more federal and state laws require that organizations protect the privacy and security of sensitive personal information in electronic form, companies increasingly pressure their information technology contractors to implement stronger data protection practices and procedures. IT contractors must be prepared to document the security of their internal processes and their employees. Contractors can even gain a competitive advantage by offering this documentation proactively.

Sophisticated customers of IT contractors often require adherence to the American Institute of Certified Public Accountants Statement on Auditing Standards (SAS) No. 70, which certifies data security safeguards. Some companies also require SAS 70 certification of IT subcontractors. In addition, IT service contracts increasingly require vendors to provide notice to their customers in the event of a security breach, such as the loss or theft of a laptop computer containing sensitive data. These clauses can require oral notification of the customer within 24 hours, with subsequent written notice. Contract terms can also require that IT service providers indemnify expenses from a data security breach, such as the cost of consumer credit reports for any affected individuals.

Customers may demand that their IT contractors conduct background checks on all employees who perform work for the customer. Some may even stipulate the type of check performed (a general credit report or a full security investigation) and request the results for specific employees. To avoid confidentiality problems, IT contractors can counter such requests by allowing their customers to define the type of background check conducted, and then certifying all employees that have met customer requirements.

Philip L. Gordon
Shareholder and Chair, Privacy and Data Protection Group
pgordon@littler.com
Peer Review Rated

Littler Mendelson P.C.

PROACTIVE PATENT STRATEGY

Although infringement litigation by "patent trolls" (who generate revenue through patent lawsuits) is highly publicized, patent litigation among active competitors is also increasing. Such recent cases as *International Business Machines Corporation v. Amazon.com, Inc.* and *Visto Corporation v. Seven Networks, Inc.* illustrate aggressive patent enforcement attempts against competitor technologies. Many companies pay large settlements to avoid the costs and uncertainty of such litigation. Others consider patent insurance, which typically has high prices and deductibles.

Seeking patent protection for their commercialized technology can help companies preserve an exclusive technology space (a good objective), but is not an effective "bargaining chip" against competitors alleging infringement. A better strategy to defend against infringement claims is to assess competitors' technological strengths and objectives and seek patent protection in areas in which competitors are most likely to invest. Such a strategy begins with an analytical report on the "patent landscape" based on public records. Given that patenting activity is a good barometer of future business activity, analyzing competitors' patent publications will reveal their technology strengths and market intentions. Such reports frequently identify technology coveted by competitors that a company otherwise would not find worthy of patent protection. Pre-emptive patents for these technologies, in addition to protection for your products, can give your company a strong bargaining position when competitors allege your practices infringe their patents.

Most companies seek patent protection for their own products. A patent strategy driven by competitive analysis can secure patent rights more likely to achieve your business objectives, making intellectual property assets more valuable.

Marc S. Kaufman
Partner, Technology & Intellectual Property
mkaufman@nixonpeabody.com

Nixon Peabody LLP

IT VENDORS AND RULE 45

Rule 45 of the amended Federal Rules of Civil Procedure may pose particular e-discovery challenges for information technology vendor companies regarding electronically stored information (ESI). Amended Rule 45 specifies that a subpoena may be used to require a person or entity to produce ESI in its ordinarily maintained form. IT vendors that have provided data management services to customers facing a subpoena under Rule 45 may themselves receive a subpoena and be ordered to produce ESI directly as part of discovery.

In-house counsel for IT companies may want to consider objecting to the production of this ESI if it was generated in the context of other litigation, such as mass tort lawsuits involving the cigarette industry, on the grounds that the subpoenaed ESI is covered by privilege. Also, counsel may object to Rule 45 subpoenas because they conflict with vendor obligations to maintain privacy of personal information under such legislation as the Health Insurance Portability and Accountability Act (HIPAA), which imposes information security requirements on external service providers handling personal health records. Even when objecting to an ESI subpoena, counsel for IT vendors must place a litigation hold on all relevant ESI to ensure its preservation. Severe sanctions are likely for failure to produce subpoenaed ESI if the court does not uphold the objection to the subpoena.

Amended Rule 26 requires opposing counsel to meet at the start of discovery to determine the ESI that must be produced. Participation in these meetings may help IT vendor counsel decide whether to contest a subpoena.

Caroline T. Pryor
Partner, Commercial Litigation
ctp@carrallison.com
Peer Review Rated

Carr Allison

"VIRAL" OR "COPYLEFT" LICENSES

The open source movement is based upon "free" sharing of source code. Open source software (OSS) users may distribute software (and charge for this service), obtain source code and change the software or use it in new free programs.

The Free Software Foundation and the Open Source Initiative approve one or both of two types of open source licenses: 1) those that license source code for distribution without imposing terms; and 2) those that require changes to be made available under the terms of the same license. The second category is a "viral" or "copyleft" license, as source code of the derived work must be shared.

The most prevalent copyleft license is the GNU General Public License (GPL), version 2, June 1991. Its key provision is in Section 2(b):

> "You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties."

Users of proprietary software models must consider the risk of OSS finding its way into a proprietary project, with the "viral" effects described above. Users must also consider that upstream parties in the licensing chain may have infringed upon intellectual property rights of third parties.

In M&A transactions, an acquirer should ask about the use of OSS in the target company's products, and assess the impact on value and the risk of third-party IP claims.

Paul E. Brace
Partner
pbrace@millerthomson.com

Miller Thomson LLP

For more information about these lawyers and their firms and to read more legal analysis on the information technology industry, please visit www.martindale.com and our Legal Articles database.

Steve Cole/Photodisc Green/Getty Images