Information Systems Frontiers 6:2, 153–160, 2004

An Overview of Leading Current Legal Issues Affecting Information Technology Professionals

Jeffrey H. Matsuura
Assistant Professor and Director of the Program in Law & Technology, University of Dayton School of Law, 300 College Park, Dayton, OH 45469, USA
E-mail: Jeffrey.Matsuura@notes.udayton.edu

Abstract. *This article provides an overview of key legal issues currently affecting information technology professionals. An understanding of the current legal issues affecting information technology development, distribution, and use can enhance the ability of information technology professionals to perform their duties. This article highlights some of the most highly visible current legal issues affecting information system operations and management. It is intended to provide technology professionals a basic understanding of today's prominent technology law issues and to help the professionals recognize their connection with those issues.*

Key Words. *DMCA, HIPAA, antitrust, trade secrets, privacy*

Law and the Information Technology Profession

Information technology professionals now frequently find themselves actively involved with a variety of legal issues. In some cases technology professionals are called upon to help facilitate compliance with legal obligations, developing and operating secure computer systems to ensure that the privacy of protected information is not compromised, for example. In other instances those professionals are involved in activities that create new challenges for the law, developers of peer-to-peer file sharing technologies, for instance. This article is intended to serve as a primer, providing technology practitioners with a basic awareness of some of the leading civil law issues they are likely to encounter today in the course of their professional activities.

This article addresses only the civil law issues of concern to technology professionals. Civil law involves the private legal rights that are enforced by one private party against another private party. Criminal law, the legal obligations that are enforced by government, are beyond the scope of coverage for this article. Instead, this article provides an overview of the private legal rights that are now most actively enforced in the context of computer technology.

Information Privacy and Computer Security

A diverse range of legal obligations associated with information privacy and computer security are now in place. In general, information privacy requirements focus on protection of personal information that can be identified with a specific individual ("personally identifiable" information). Information privacy obligations often carry requirements for computer system security, as the protected information is commonly stored and processed on computers. In this way, information privacy and computer security are interrelated.

Several different privacy regulations targeted to protect specific forms of personal information have been enacted at the federal level in the United States. For example, the Health Insurance Portability and Accountability Act ("HIPAA") established privacy requirements regarding personally identifiable health and medical information. The HIPAA requirements are enforced by the federal Department of Health and Human Services, and they apply to all organizations that collect or process personal health care information.

Another example of targeted federal privacy legislation is the Gramm Leach Bliley Act. The Act establishes privacy protection for certain forms of personally identifiable information collected by financial

services institutions individual consumers. Gramm Leach also imposes notice requirements associated with the transfer of personal financial information. Regulations developed under the Act are enforced by a variety of federal organizations, including the Department of the Treasury and the Securities and Exchange Commission.

HIPAA and the Gramm Leach Bliley Act regulations also establish security requirements for computer systems that process information protected under those regulations. Computer security is a critical aspect of information privacy, thus privacy requirements are commonly linked to security obligations. Organizations that must comply with HIPAA or Gramm Leach requirements rely on their information technology professionals to ensure compliance with those legal obligations.

Other countries apply information privacy requirements that are more stringent than those enacted at the federal level in the U.S. For example, the European Community and Canada have implemented sweeping information privacy protections, in contrast to the targeted approach applied in the U.S. Information system professionals working for organizations that do business in Europe or other jurisdictions with comprehensive information privacy laws play a key role in compliance with those legal obligations.

Some jurisdictions have now implemented notification requirements when the integrity of personal information has been compromised. California's statute, SB 1386 for example, requires notice to individuals when their personal information has been compromised. Technology professionals working for organizations that fall within the scope of the California statute are actively involved in preventing unauthorized access to personal information which invokes the notification requirement. They also play a key role in identifying when information has been compromised, thus triggering the notice requirement of the law.

Legal issues associated with the integrity of information have a significant impact on computer professionals. A leading example of this connection is provided by the Sarbanes-Oxley Act, federal legislation in the United States. Generally, Sarbanes-Oxley places requirements on senior management of publicly-traded companies to take personal responsibility for disclosure and accuracy of financial information of their companies. The information disclosure and verification requirements of Sarbanes-Oxley have a significant impact on information system professionals. Public companies now require more rigorous financial record-keeping, auditing, and reporting. These additional legal compliance obligations place an extra set of demands on corporate computer systems. Information technology professionals who develop, maintain, and manage those systems are thus at the center of Sarbanes-Oxley compliance efforts.

Information technology professionals have a significant role to play in compliance with legal requirements associated with information privacy and integrity, and the computer security obligations associated with management of the protected information. Those professionals are called upon to devise information systems that provide the requisite levels of privacy and security. They are also the people who will bear the burden of managing the operations of the systems to ensure compliance, and of developing and implementing remedial measures when compliance problems arise.

Trade Secrets and Proprietary Information

Information systems are repositories for vast amounts of confidential information. The law provides for protection of confidential material as trade secrets. Theft of trade secrets is illegal and can be addressed through tort law claims or claims raised under other statutory provisions (such as the federal Economic Espionage Act). Virtually any form of information, knowledge or know-how that provides its owner with a commercial advantage derived from the fact that the owner has access to the material and its competitors do not, will qualify for trade secrets protection.

To preserve trade secrets protection under the law, however, the owners of the secrets must act prudently to safeguard the confidentiality of the secrets. Trade secrets law will not provide a remedy if the secrets are obtained without permission and the owner of the secrets failed to exercise reasonable care to protect their secrecy. In addition, trade secrets law does not protect an owner of trade secrets from independent discovery of the information by another party or from a party who obtains the secrets lawfully from a different source.

Information system managers frequently encounter principles of trade secrets law as they face the task of managing computer resources in a manner that facilitates protection of confidential material. Their ability to devise and operate secure computer systems is critically important to the ability of their organization to protect the confidential material and to preserve trade

secrets rights that are enforceable if confidential material is compromised. An information system that does not provide effective security and oversight for confidential material can contribute to the loss of that material, and it can also lead to the loss of trade secrets legal rights.

Information technology professionals also commonly face trade secrets issues because they are generally among the personnel in an organization who are granted access to the organization's trade secrets. Technology professionals are often required to enter into confidentiality or non-disclosure agreements with their employers or clients, as part of the trade secrets protection practices of those organizations. A basic understanding of trade secrets law is thus important for computer professionals, as they are often personally bound by obligations imposed by that field of law.

A legal concept related to trade secrets protection that also affects many information technology professionals is a non-competition agreement. The law will enforce limited contractual agreements in which an individual promises not to compete against the other party to the agreement. Technology professionals are probably most familiar with this type of agreement in the context of employment contracts, where the employee agrees not to compete against the employer during the term of employment, and generally for some limited period after the employment relationship ends.

The enforceability of non-competition agreements varies widely from jurisdiction to jurisdiction. Some jurisdictions, such as California, are extremely reluctant to enforce non-competition agreements, while other jurisdictions are more willing to honor them. All jurisdictions, however, try to enforce these agreements as narrowly as possible, particularly in the context of an employee who has made a commitment not to compete. Narrow scope of enforcement is generally preferred as there is a common assumption that commercial competition serves the public interest, those contract arrangements that reduce that competition do not provide the ideal business arrangement. When the agreement involves a former employee, the desire to interpret the scope of the agreement narrowly is even stronger, as courts recognize that the non-competition agreement limits the ability of the individual to earn a livelihood.

Non-competition agreements generally define the boundaries within which the party bound by the agreement promises not to compete. Those boundaries are generally defined in terms of type of activity, time period, and geographic region or market. Thus for example, a non-competition agreement for a software developer might indicate that the developer agrees not to develop a specific type of software for sale to a specific set of customers in a certain geographic region for a defined period of time. The enforceability of that agreement will be substantially dependent on the reasonableness of the agreed upon restrictions.

Trade secrets law is significant to information systems professionals as they play a key role in protecting those secrets and in preserving the ability of their organizations to invoke the remedies that the law provides. In addition, technology professional commonly have a direct personal interest in trade secrets law. As they are often personally bound by contractual agreements associated with use of confidential material, they have a clear personal stake in understanding the basic principles of this field of law, in order to protect their own interests.

Intellectual Property

Intellectual property law is most commonly defined as the legal rights associated with patents, copyrights, trademarks, and trade secrets. Information technology is integrally involved in issues of intellectual property development and use. These legal issues arise in the context of computer equipment, computer software, and online content. Intellectual property law issues have an important impact on actions of information system professionals, as they define the scope of rights of access and use to materials that are developed and obtained by those professionals.

One of the most visible intellectual property law issues involving information technology is that of establishing effective management of digital media rights. The most visible controversies associated with management of digital media rights are associated with online music distribution. Dramatic expansion in the use of the MP3 format and peer-to-peer (P2P) file-sharing systems led to a significant increase in the scope of unauthorized distribution of copyrighted music.

In response to this upsurge in digital music piracy, the music industry has emphasized two initiatives that have significant impact on the information technology community. The first is to encourage development and use of new technologies that control access to digital sound recordings and facilitate payment for such access. The second impact is active litigation to enforce their copyrights, with much of that litigation presented

under the terms of the Digital Millennium Copyright Act (DMCA), with particular emphasis on the anti-circumvention provision of the DMCA. The campaign of aggressive litigation by the music recording industry to enforce copyrights under the DMCA has been largely directed against individual music users, including highly visible examples of lawsuits against both the elderly and the very young.

The DMCA's anti-circumvention provision is of particular significance to the information technology community, as it has been applied to restrict the development, distribution, and use of certain forms of decryption technology. The provision prohibits creation, distribution, and use of technologies that can override, work around, or otherwise circumvent systems that are intended to protect copyrighted material from unauthorized access. The provision is controversial in part because it can be invoked against technologies that have not actually been used for copyright infringement, but merely have the capability of enabling infringement. Technology professionals have expressed concerns about this provision as it can be invoked against developers of technologies with circumvention capabilities, even if the developer did not directly use the technology to infringe on any copyrighted material. The anti-circumvention provision thus provides a legal action against individuals associated with technology that has copyright circumvention capability, even if there is no evidence that the individuals actually used the technology to infringe on any copyright.

The rapid development of the open source licensing model for various software products provides another important intellectual property law topic. Open source licenses generally permit the licensee to access and to modify the source code for the licensed software. In exchange for that broad grant of rights, open source licenses commonly require the licensee to make the original software and all modifications made by the licensee available on an open source basis.

A major controversy has been sparked in the open source community by the various lawsuits and claims raised by the SCO Group. SCO Group claims proprietary rights as to code elements that have been integrated into the Linux open source product. Based on that claim, SCO Group has challenged open source software developers and users, alleging that it is entitled to compensation for a wide range of Linux applications. The SCO Group litigation illustrates a significant challenge associated with open source management. It is often difficult to manage different ownership rights when computer programs integrate open source and proprietary elements. Much of the burden for monitoring those different license terms and for ensuring compliance with the terms of the varied licenses rests with information systems managers.

The SCO Group litigation also underscores the fact that information technology professional in all organizations involved with open source products should understand the terms of the open source licenses and should play an active role in license compliance. SCO Group is prepared to litigate its claims against software developers who integrate the open source code in question into their products. It is also apparently willing to litigate against all parties who use the programming in question, including manufacturers of computer equipment that runs the programming and users of products that contain the programming. This controversy illustrates the importance of information technology professionals in all organizations involved in the computer industry (software developers, hardware manufacturers, and computer product users) understanding the basic principles of the open source model, as licensing disputes associated with the base open source product has important legal implications for all parties associated with the product.

Another intellectual property issue of significance in the field of information technology is the debate associated with software and business method patents. In the United States, patents can be obtained for both computer programs and methods of conducting business. Other countries are, however, far less open to both software and business method patents. Some highly visible software and e-commerce business method patent disputes drew significant attention to the debate over the appropriateness of those classes of patents.

For example, litigation initiated by Amazon.com against Barnesandnoble.com underscored conflicting perceptions as to e-commerce patents. One school of thought viewed these patents to be important motivation for continuing investment in new inventions and valuable insurance against infringement actions brought by other patent owners. Others in the e-commerce industry saw the patents as impediments to innovation, blocking development of legitimate and helpful applications that make use of the patented methods.

Trademark law has been actively invoked in the context of domain names, metatags, and online keyword searches. Trademarks of other parties incorporated into Internet domain names or included in Web

page keywords for the purpose of attracting search engines have been characterized by courts as trademark infringement. Trademark law in the United States was amended to establish the civil law violation of "cybersquatting," the process of registering another party's trademark within an Internet domain name, in bad faith.

Information technology professionals have a significant stake in these current intellectual property law issues. At one level, computer professionals are often developers of intellectual property, and in that role, they have an interested in the establishment and enforcement of intellectual property law rights that assert control over access to and use of the material they create. At the same time, information technology professionals are often commonly significant users of intellectual property. In that capacity, they have a direct interest in the preservation of open access to intellectual property, subject to reasonable terms and conditions.

Property Rights

Civil law recognizes and enforces rights of ownership and control over forms of property in addition to intellectual property. In various contexts, courts have been willing, at least in part, to treat computer equipment and computer content as personal property. To the extent that computers and their content are property, traditional property law principles such as trespass have been applied as a means to control access to the equipment and content. These property law concepts are distinct from intellectual property law theories, such as copyright, that have also been applied to computer content.

Courts have been asked to apply property law principles and concepts to computer hardware and content. For example, in a dispute with a former employee, Intel persuaded a California court that bulk e-mail messages constituted trespass on Intel property (its e-mail servers). Courts have also been willing to find access to data stored on a server to constitute trespass.

Antitrust, Competition, and Commercial Law

Civil law seeks to protect the vitality of competitive commercial marketplaces. Laws aimed at preserving fair commercial competition are generally described as antitrust and competition law. In addition, the law is concerned that commercial transactions (e.g., sales) are fair and effectively enforced. The law of contracts and commercial transactions provides the civil law foundation for protection of the commercial marketplace.

Perhaps the leading aspect of antitrust law in the information technology sector in recent history is the litigation against Microsoft brought by U.S. federal and state authorities. Microsoft was found guilty of having engaged in anti-competitive conduct in order to extend its monopoly in the personal computer operating system marketplace. During the course of the Microsoft litigation, important principles of antitrust law were applied for the first time to the information technology marketplace.

The Microsoft litigation demonstrates that the basic principles of antitrust law will be applied to anti-competitive conduct associated with computer software and other forms of computer technology. The litigation also illustrated the extent to which limitations on access and rights of use for information technology products can have significant adverse effects on competition.

Antitrust controversies associated with companies such as Rambus illustrate that market power can be based entirely on control over a technological standard. Ability to set and control technical standards creates market power which can be exercised in anti-competitive ways. Accordingly, antitrust regulators now pay substantial attention to the processes used to develop and implement technical standards. This regulatory focus is important to technical professionals as they are often actively involved in the development of those standards.

Among the antitrust lessons to be learned by information technology professionals is the need to ensure that technology standards and practices are developed based on defensible technical and commercial grounds. Technical standards and business practices that are motivated by sound technological or business reasons are generally lawful. When those standards and practices are motivated by a desire to reduce commercial competition, however, they are likely to be incompatible with the basic requirements of antitrust and competition law.

Consumer Protection

The dramatic growth in online commerce has raised significant consumer protection law issues. The Federal Trade Commission and state consumer protection

authorities are now highly active regulating electronic commerce transactions. One of the leading consumer protection subjects is e-commerce fraud. The FTC and other consumer protection agencies now have as a point of emphasis action against fraudulent and deceptive sales practices by online retailers and by individual seller in online auction transactions.

Another area of emphasis for consumer protection authorities is oversight of commercial transaction terms. Consumer authorities thus monitor terms of click-through agreements, as well as electronic contracts and terms of service applied to e-commerce transactions. Regulatory oversight of online consumer agreements generally addresses both the content and the form of those agreements. Consumer protection authorities are concerned that the terms of online consumer agreements be reasonable and fully disclosed. They are also eager to ensure that the terms of the agreements are presented in a manner that facilitates consumer understanding and verifies clear intent by the consumer to accept the terms of the agreement and transaction.

Consumer protection authorities also focus on the information privacy and transaction security practices of businesses engaged in electronic commerce. E-commerce retailers are expected to apply reasonable security and privacy policies and practices. Businesses that either fail to adopt such standards or do not meet the standards they present to consumers face potential charges of deceptive trade practices from consumer protection authorities.

Much of the burden of devising and operating electronic commerce systems that satisfy consumer protection requirements falls on information system professionals. For example, information technology specialists face the task of ensuring that the functional capabilities of the e-commerce transaction systems are consistent with the representations regarding those capabilities that are made to consumers and are relied upon by those consumers. In large measure, the ability of electronic commerce operations to comply with consumer protection requirements is controlled by information system managers.

Export Controls

Federal law in the United States restricts the international distribution of technology and knowledge that have potential military applications. International export of material subject to these controls requires prior approval and licensing by federal authorities. Export controls have been the subject of attention in the information technology industry particularly when applied to computer equipment and encryption software. Computer technology is regulated, for export control purposes, by computational speed. Encryption technology is regulated based on the sophistication of the encryption key necessary to decrypt the protected content.

Export controls are federal rules that have substantial potential impact on information system professionals. Some of the most challenging export control issues are associated with computer equipment and software. The increasingly widespread presence of significant computing power in many different devices, including consumer electronic, appliances, and even toys, makes compliance with export controls associated with computer equipment a major challenge. The global nature of computer networks and the increasing demand for greater encryption protection make export control compliance for encryption technology another difficult information system management undertaking. In today's technological and commercial environment, export control compliance in the world of information technology is perhaps more difficult than compliance management for any other form of technology. Information system professionals confront the task of ensuring such compliance.

New Technologies and Applications

Continuing development of new technologies and new applications for existing technologies present significant challenges for civil law principles. For example, software products such as "spyware" have generated legal controversy. "Pop-up" advertising systems associated with Internet browsing provide another example of a new technological application that raises legal debate. Legal issues regarding privacy, unfair competition, and property rights have been raised in response to increased use of spyware and pop-up advertising systems.

Distributed computing systems and applications provide another example of computing advances that are raising new legal issues. Software that enables an outside party to harness unused computing capability of individual computers on a network is beginning to attract legal attention. The concept involves using the computing resources of many different client

computers on a network, when the owners of those computers are not using them, and directing those aggregated computing resources toward a specific application. When software that enables this distributed computing capability is integrated into software that is made available at no charge to end users (in much the same way that spyware has been distributed in the past), the capability can be spread to a large number of individual computers quickly. Distributors of the software can thus have access to significant distributed computing power fairly quickly. Some industry observers, however, are now raising concerns as to whether informed consent for this arrangement has been obtained from the end users, and whether this type of system constitutes some form of property law and privacy violation.

Information technology professionals continue to develop new systems and new applications. Many of those innovations raise novel legal issues, while others force traditional legal concepts to adapt to new circumstances created by the innovations. In this way, information technology professionals drive virtually all of the legal issues associated with computers and computer use. There is every reason to believe that this dynamic process will continue into the foreseeable future. Technology professionals seek and create technical advances, and each of those advances has potential legal implications.

Conclusion

Information technology professionals have a significant stake in the various legal challenges and controversies associated with computers and online activity. Computer professionals are frequently called upon to develop and implement technical means to resolve some of these legal issues. Under some circumstances, the creativity and innovativeness of those professionals create new challenges for laws and legal institutions. We also see that information system professionals play critical roles in the ability of organizations to comply with virtually all of the legal obligations associated with online commercial activities.

Information technology professionals are thus essential contributors to all sides of virtually every technology law issue. They contribute to the creation of those issues. They assist in the development of resolutions for those issues. Finally, they are largely responsible for compliance with the legal obligations that develop in response to those issues. Seen from this perspective, it appears that information technology professionals play a role in technology legal matters that is as significant as that played by legal professionals. In such an environment, awareness of the legal issues and a basic level of understanding of those issues are valuable assets for technology professionals. A working knowledge of key legal challenges associated with information technology is now an important addition to the skill set of information system professionals.

References

A&M Records, Inc. v. Napster, 239 F. 3d 1004 (9th Cir. 2001).
Amazon.com v. Barnesandnoble.com, 239 F.3d 1343 (Fed. Cir. 2001).
Anticybersquatting Consumer Protection Act, 15 U.S.C. 1125.
Digital Millennium Copyright Act, 17 U.S.C. 1201 et al.
eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000).
Health Insurance Portability and Accountability Act, Pub. Law 104–191, 1996, at http://www.hipaadvisory.com
Intel corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Ct. App. 2001).
In the Matter of Rambus, Inc., FTC Complaint, Docket No. 9302 (2002), at http://www.ftc.gov/os/2002/06/rambuscmp.htm
Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D. N.Y. 2000).
United States v. Microsoft, 97 F. Supp. 2d 59 (D.D.C. 2000).
United States Export Control Regulations at http://www.bxa.doc.gov.
Universal Studios v. Reimerdes, 2000 U.S. Dist. LEXIS 11696.

Jeffrey H. Matsuura is Assistant Professor and Director of the Program in Law and Technology at the University of Dayton School of Law. Courses taught by Professor Matsuura include: Cyberspace Law, Licensing Intellectual Property, Protection of Computers and Software, and Intellectual Property Law. He is the author of the following books: *Security, Rights, and Liabilities in E-Commerce; A Manager's Guide to the Law and Economics of Data Networks*; and *Managing Intellectual Assets in the Digital Age*. He is also co-author of the book, *Law of the Internet*, and he is the author of numerous technology law articles. Professor Matsuura lectures internationally on the legal and public policy implications of technology and he served as a commentator on law and technology for the National Public Radio program, "The Law Show." He has more than 20 years of experience representing clients in the telecommunications, computer, digital media, and space industries, including: The Discovery Channel, MCI Communications

Corporation, COMSAT Corporation, and TELE-TV. Professor Matsuura has earned degrees from Duke University, the University of Virginia, and the Wharton School at the University of Pennsylvania. He is Of Counsel with the technology law firm, the Alliance Law Group, in Vienna, Virginia. Professor Matsuura has also served as an advisor to the Virginia General Assembly's Joint Commission on Technology and Science and to the National Taskforce on Knowledge and Intellectual Property Management.