

WILLCOX & SAVAGE

TECH LAW LETTER



INTRODUCING THE NEW WILLCOX & SAVAGE TECH LAW LETTER

Timothy J. Lockhart

Group Leader, Intellectual Property Group



Thank you for taking time to review our "Tech Law Letter." This issue is the first of what will be a regular series of newsletters on the latest developments in intellectual property and technology law. We will report on key issues related to acquiring, protecting, and licensing rights in patents, trademarks, copyrights, and trade secrets. In addition, we will cover important developments in related areas such as communications, government contracts, and privacy. We hope you enjoy reading the "Tech Law Letter," and we welcome your questions and comments concerning any of the articles in it.

Intellectual Property (IP) Seminar Series Continues on October 6, 2004

The IP Group held its first seminar in the series on June 9 at the new Town Center City Club. The Group's attorneys presented overviews of IP, privacy and patent law. The next session will be held on October 6 at the Norfolk Airport Hilton from 8:00am-10:00am, and will cover licensing your IP, protecting your IP rights in bankruptcy, and other IP matters. If you're interested in attending our next seminar please register on-line at <http://www.willcoxsavage.com/nep/seminars.html>. As seating is limited you will receive registration confirmation.

HOW DOES YOUR COMPANY'S DATA SECURITY MEASURE UP? DEVELOPING LEGAL STANDARDS IN A BRAVE NEW WORLD.

Leslie F. Spasser



In today's competitive world, almost every company, whether online or "brick and mortar," maintains databases of information about their customers. They use this information for a variety of purposes – from direct marketing, to the development of customer loyalty programs to simple billing and order fulfillment. Maintaining customer information and using it to simplify billing and payment processes or provide better customer service can benefit consumers and enhance the bottom line of a business. Yet as lawmakers, enforcement agencies and plaintiffs' lawyers focus on the dangers of identity theft and cyber-security in general, many companies place themselves at risk by ignoring the growing responsibility they have to maintain such data in a secure manner and protect it from unauthorized intrusions.

A few questions face today's in-house counsel. First, what level of security are companies legally obligated to provide? Second, what practical steps should companies take to minimize liability?

These questions are posed in a shifting legal environment and one in which there may be developing a set of government-endorsed security standards or "best practices" that companies ignore at their own risk. During the past few months, a number of government agencies, including the Department of Homeland Security, the Federal Trade Commission and the House Committee on Government Reform have issued documents identifying best practices for the private sector to use in addressing cyber-security. These statements likely will become de facto standards for baseline

CONTINUED ON PAGE 2

acceptable security programs. Companies that ignore these standards risk being viewed as negligent in the event that a security breach occurs; and companies that implement the recommended practices may be able to use evidence of such compliance to reduce their potential liability in the event of a security breach.

Existing laws governing data security also provide insight into developing standards. Although these laws tend to be industry-specific (such as the Health Insurance Portability and Accountability Act to the health care industry, and Gramm-Leach-Bliley Act to the financial services industry), the security practices and processes they mandate could apply to almost any business.

Recent enforcement actions by the FTC against Microsoft Corp., Eli Lilly and Company, and Guess? Inc. likewise indicate the development of an accepted set of security standards. In these actions, the FTC targeted alleged misrepresentations about the level of security provided by the defendant companies' websites or products. However, the resulting consent decrees required the defendants to implement security programs that could apply more generally (these consent decrees can be found on the FTC website at www.ftc.gov).

Further, certain states are enacting laws that address information security. In 2003, California enacted a law requiring the prompt disclosure of any breach of a network security system that results in the acquisition of unencrypted personal information by an unauthorized person (Cal. Civ. Code § 1798.82). The law does not mandate specific processes for maintaining information security, but it has the effect of penalizing businesses that do not encrypt sensitive information, such as social security numbers, bank account numbers and credit card numbers. This state law echoes similar statements by the FTC and, in response to increasing incidences of identity theft, California Senator Feinstein currently is sponsoring a bill to impose similar requirements at the federal level.

It is important to note that most laws and statements issued by the government addressing security do not require specific solutions. Rather, they view security as a "process, not a product" and set forth regimes requiring companies to address security in a flexible, ongoing manner. For instance, in the Eli Lilly, Microsoft and Guess consent decrees, the FTC required each respondent to "establish and maintain an information security program" that included, *inter alia*, the following elements:

- *The designation of appropriate personnel to coordinate, oversee, and be accountable for the program;*
- *The identification of reasonably foreseeable internal and external risks to security;*

- *The requirement to address such risks by*
- *creating an appropriate employee training and management program;*
- *evaluating information systems for the processing, storage, transmission, and disposal of information; and*
- *designing and implementing reasonable safeguards to prevent and respond to attacks, intrusions, or other systems failures.*
- *Regular testing and monitoring of the effectiveness of the safeguards.*
- *The evaluation and adjustment of the information security program in light of the results of the testing, changes to respondent's operations or business arrangements, or other circumstances that may have a material impact on respondent's information security program.*
- *The institution of regular third-party audits of the program.*

The recent joint statement issued jointly by the FTC, the National Cyber Security Alliance and the Council of Better Business Bureaus provided more specific guidance. The organizations issued "tips" for businesses to use to keep their computer systems secure, and recommended the following:

- *Maintain a password protection program.*
- *Use virus protection software.*
- *Install firewalls.*
- *Use security patches issued by software vendors.*
- *Back up your data.*
- *Routinely check for suspicious activity.*

We hope you find our newsletter informative and useful. If there is a topic you would like covered, or would like to receive this newsletter via e-mail, please contact Michelle Shearon at 757-628-5631 or e-mail mshearon@wilsav.com. This publication is provided for general purpose information. It is not and should not be used as a substitute for legal advice. Copyright 2004 Willcox & Savage, P.C.

- *Note the risks of file sharing.*
- *Consider buying encryption software (to protect data on your network in the event an intruder manages to break your systems)*
- *Educate your employees by developing and enforcing a company-wide computer and physical security policy and holding routine briefings and updates for employees on these policies as well as on new security threats, corrective measures and incident reporting procedures. See www.ftc.gov/opa/2004/04/cybersecure.htm.*

While the guidance discussed above is informative, it does not resolve legal uncertainty created by the absence of specific statutes governing general database security. So the question becomes whether there is an implied duty of care requiring companies to secure customer information. Under this theory, a company that fails to take “reasonable steps” to ensure security could be deemed negligent. It is difficult to see the law requiring companies to provide ironclad security and, in fact, the House’s Committee on Government Reform recently issued an initiative to provide a safe harbor from liability to private sector companies who develop coherent cyber-security programs. See “Incentives-Liability/Safe Harbor Recommendations,” found at <http://reform.house.gov/UploadedFiles/Incentivesposter.pdf>. However, the law may evolve in a direction that imposes liability on companies that (a) do not implement reasonable policies to assess and address the flaws in their systems; (b) become aware of security vulnerabilities but choose not to take reasonable steps to cure them; or (c) fail to implement processes to notify consumers in the event of security breaches.

GLB, HIPAA, and the FTC statements and consent decrees incorporate the concept of “reasonableness” in identifying foreseeable risks and taking appropriate precautions to address them. By its nature, reasonableness will be assessed on a case-by-case basis in light of the specific details of the breach and the business at issue. However, there are indicia of reasonableness that courts or regulatory agencies likely will use as benchmarks. Industry standards, available security tools and developing consensus on the components of an appropriate security program (which may be facilitated by the government as it pursues cyber-security initiatives) will become important points of reference when assessing whether a company has taken reasonable steps to identify and address security risks.

As these broadly applicable legal standards are developing, companies can take steps to minimize their exposure to security breaches by (a) implementing a security program (using the components outlined by the FTC, HIPAA, GLB and the National Cyber Security Partnership as references);

(b) developing processes for notifying customers in the event of certain types of security breaches; and (c) ensuring that contracts with third-party vendors who may access or process a company’s customer information contain adequate security protections.

Implementing an effective security program minimizes the risk of a security breach by creating awareness within a company of vulnerabilities and putting in place safeguards and monitoring processes to protect key assets. Further, companies that implement and maintain effective security programs are more likely to be deemed to have taken reasonable steps to maintain security in the event of a breach – which may influence liability and reduce the measure of damages assessed in the event of a breach.

Developing processes by which customers are informed in the event of a security breach also is essential – not only to comply with the California law discussed above, but also to reduce exposure to claims of unfair practices (such as those sparking the FTC consent decrees). Most companies have privacy policies notifying customers what information they collect and how they use and disclose it. It is equally important to implement a security policy – and an internal process for determining when a breach has occurred, what information, if any, has been compromised, and what disclosures, if any, are required. For instance, if unencrypted credit card numbers have been exposed and there is an ongoing risk of identity theft and financial harm to customers, it probably is necessary to notify affected customers immediately so they can take measures to protect themselves. On the other hand, if encrypted information is accessed but not compromised, there may be no harm to consumers and, therefore, no reason to disclose. However, a company is best protected if it sets up a process by which such situations are evaluated and addressed case by case.

Finally, to the extent a company uses third parties to process, store or otherwise access its customer information, the company must ensure that the vendor is contractually bound to maintain that information in a secure manner that meets industry standards. For especially sensitive information, such as financial information or social security number, it may be a good idea to require third-party vendors to use specific techniques, such as encryption, in the storage and transmission of that information.

In summary, the legal environment surrounding data security is evolving. However, by implementing a security program, putting in place customer notification policies and ensuring their third-party contracts contain adequate security protections, companies can mitigate their exposure and continue to maintain and use customer information to enhance their customers’ experience and their own bottom line. ■

ARE YOU IN VIOLATION OF CAN-SPAM? FOUR SIMPLE RULES OF E-MAIL SOLICITATION.

Kevin W. Grierson



The CAN-SPAM Act, which went into effect January 1, 2004, was designed to stem the flood of e-mails, many with pornographic content, that come from bulk e-mailers, or "spammers." However, the Act applies to all commercial e-mail soliciting business for the sender, not just high volume distributors.

Although the CAN-SPAM does not permit suits by individual recipients of unwanted e-mails, Internet service providers can sue (and a few already have sued) senders of unsolicited e-mails if their customers complain, and the Department of Justice has the authority to enforce criminal sanctions. And since legitimate businesses are more likely to be easily located, they may be more tempting targets than the spammers the Act was intended to stop. Therefore, even if you send out e-mail advertisements only on occasion, it's important to comply with the law.

Here are a few simple rules to follow for any commercial e-mail solicitations, which were recently published by the FTC:

- *Don't change "header" information. Your e-mail's "from," "to," and routing information should not be changed or disguised in any way.*
- *Use accurate subject lines. Don't use subject lines that would mislead the recipient as to the true nature of the e-mail. Clearly identify your e-mail as an advertisement.*
- *Provide a valid online opt-out method, and honor requests to opt out of your solicitations. The law requires you to honor the request within 10 days of receiving it. You can create a menu of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end all commercial messages.*
- *Include a valid physical postal address. Because some spammers have reportedly used unsubscribe requests to verify the validity of e-mail addresses, some recipients may wish to ask to be removed from your list by regular mail.*

The CAN-SPAM Act does not put an end to legitimate e-mail solicitations and internet commerce, and by following the above rules, most companies will find compliance easy. A routine check that the rules are being followed can prevent litigation and keep potential customers from being annoyed. Banishing the spammers completely may not be possible, but the FTC has taken the steps to limit their e-mail reach. ■

ABOUT THE ATTORNEYS

Timothy J. Lockhart is the Group Leader of the IP Practice and is also a Captain in the U.S. Naval Reserve. Tim brings over 14 years of legal experience working in both the public and private sectors. His practice focuses on trademark and copyright counseling, registration and enforcement, software and technology licensing, e-commerce and other web-related agreements, trade secret protection and IP litigation, arbitration and mediation. Tim is also actively involved with the International Trademark Association (INTA), which is an organization of more than 4,500 trademark owners and professionals from over 180 countries. He has co-chaired a subcommittee of the International Trademark Association and frequently publishes articles on developments in U.S. and international trademark law. He joined Willcox & Savage in 2002 from Hogan & Hartson in Washington, D.C. He received his J.D., *cum laude*, from Georgetown University.

Leslie F. Spasser has practiced in the area of cable television and communications law and policy since 1994, representing a diverse group of clients that has included large cable television companies, broadcast television stations and cable television programmers. She has been with Willcox & Savage since September 2003. Prior to joining our firm she served as in-house counsel and privacy advisor for Cox Communications, Inc. for several years, focusing on privacy and technology law. Prior to her work with Cox, Leslie was a partner with an antitrust law firm in New York City, where she represented clients in the cable, publishing and online services industries. She received her J.D. from New York University School of Law.

Kevin W. Grierson has been practicing law for 12 years, focusing on patents, trademarks and other intellectual property matters. He is registered as a patent attorney with the U.S. Patent and Trademark Office and currently serves on the Board of Directors of the National Association of Patent Practitioners. He frequently publishes and speaks on patent and other IP issues. He received his J.D. from the University of Virginia.

On June 22 Willcox & Savage's IP Group hosted the first INTA Roundtable ever held in Hampton Roads. This event, attended by representatives of several local businesses and law firms, focused on policies and procedures for managing portfolios of U.S. and international trademarks. Tim Lockhart and Kevin Grierson co-chaired the Roundtable, and they, along with Marshall Martin of the IP Group, shared their experiences from attending this year's INTA Annual Meeting, which was held in Atlanta in May. The world's largest trademark organization, INTA consists of over 4,500 trademark owners and professionals from over 180 countries. For more information about INTA, visit the association's web site at www.inta.org.

INADVERTENT GRANT OF UNLIMITED RIGHTS IN PREEXISTING WORKS DELIVERED TO FEDERAL GOVERNMENT

Timothy J. Lockhart

Group Leader, Intellectual Property Group

Contractors delivering software and other copyrightable works to the federal government can inadvertently give the government unlimited rights in preexisting works if they do not follow the proper procedures for providing such deliverables. In January 2004 the U.S. Court of Federal Claims ruled for the first time, in *Ervin and Associates, Inc. v. United States*, that a contractor's delivery of preexisting works can grant to the federal government unlimited rights in those works even though they were not developed pursuant to the contract. Under the Federal Acquisition Regulation ("FAR") "Rights in Data-General" contract clause the government's rights extend even to disclosing such works to the contractor's competitors.

The *Ervin* case underscores the importance to contractors of seeking legal advice in the area of intellectual property when negotiating an agreement with the federal government. This fact holds true for experienced as well as inexperienced contractors, as the government holds experienced contractors to a higher standard when evaluating whether they knew or should have known of the correct procedures to follow with copyrighted works and other intellectual property delivered under a contract.

Ervin's contract called for the company to review and analyze annual financial statements submitted to the U.S. Department of Housing and Urban Development ("HUD") by the owners of approximately 16,000 HUD-insured and -held loans on multifamily apartment projects. In its response to HUD's request for proposal Ervin described a "series of currently existing interrelated database systems which contain data elements and text and are linked together to create sophisticated analysis for [a] portfolio of loans" (emphasis added).

The contract that Ervin received from HUD contained the federal government's standard "Rights in Data-General" clause. That clause provides that the government acquires unlimited rights, including an unlimited copyright license, in all data (including software) delivered under the contract unless, in the case of preexisting data, the relevant government contracting officer ("CO") agrees otherwise.

Ervin admitted that it had never asked the CO if HUD would agree to accept the preexisting databases without asserting unlimited rights to them. However, Ervin claimed that it had notified other HUD employees who were in a position to raise the issue with the CO and that the CO

"either knew or should have known of Ervin's contention" that the government was not acquiring unlimited rights in those databases.

The court rejected Ervin's arguments, ruling that "in light of Ervin's representations regarding its experience as a government contractor with a significant prior working relationship with HUD . . . it is Ervin that knew or should have known of the requirement to inform the CO directly of any issues regarding the contract." Moreover, the court stated that "if there were any questions regarding the applicability of the 'Rights in Data-General' Clause, one would expect that an experienced government contractor, like Ervin, would make an inquiry, particularly in light of Ervin's view that the [databases in question], components thereof, and all resulting output was proprietary."

In the court's view, the FAR required Ervin either to withhold the preexisting data after identifying it and furnish newly created data in its place or to affix to the preexisting data "limited rights" or "restricted rights" notices. Ervin did neither of these things, instead claiming that its oral statements, letters, and e-mails to a variety of other HUD officials provided sufficient "limited rights" notice under the "Rights In Data-General" clause. But the court ruled that because "these communications did not comply with the manner of notice prescribed by FAR . . . the Government . . . acquired 'unlimited rights' in all technical data and computer software delivered under the terms of the . . . Contract. In short, Ervin's warnings were both too late and too little." ■

WILLCOX SAVAGE

How to reach our attorneys

Timothy J. Lockhart

757-628-5582 tlockhart@wilsav.com

Marshall B. Martin

757-628-5605 mbmartin@wilsav.com

Leslie F. Spasser

757-628-5588 lspasser@wilsav.com

Kevin W. Grierson

757-628-5603 kgrierson@wilsav.com

MANAGING OPEN SOURCE SOFTWARE

Kevin W. Grierson

As Linux “open-source” software becomes more popular, particularly for servers, many businesses are thinking of adding open-source software to their networks. Because the source (or human-readable) code for open-source software is publicly available, such software can be maintained and possibly improved by all users, not just its developers. Thus, many people consider open-source software preferable to proprietary software, for which users must usually rely on the developer to fix bugs or provide upgrades, often at additional cost.

Contrary to popular opinion, open-source software is not necessarily free: companies such as Red Hat charge for support, the media on which the software is provided, and supporting documentation. Also, such software is not necessarily in the public domain; it is usually distributed with a license that, although permitting unlimited copying, has important restrictions on how the software can be used. In particular, under the General Public License (“GPL”), which governs Linux and many Linux-based applications, software that is “derived from the [open-source] Program or any part thereof . . . [if published or distributed, must be] licensed as a whole at no charge to all third parties under the terms of th[e] License.”

For that reason certain developers have labeled software distributed under an open-source license, particularly the GPL, to be “viral software” that “infects” proprietary code, not in the manner of a malicious virus but rather in the sense of converting all of that code into open-source software. Such developers take the position that any program incorporating open-source software in whole or in part may not be distributed as proprietary software. Those developers have warned users of open-source software that any code they write for their own purposes will, pursuant to the open-source license, subsequently be

freely available to third parties for their use, modification, copying, and redistribution.

However, this view of open-source software does not mean that a proprietary program that simply runs on an open-source software operating system (for example, a proprietary word-processing program that runs on Linux) will be “infected.” If there are no modifications to the open-source program and if it is not embedded within a proprietary program, the terms of the open-source license will not apply.

Still, the foregoing warnings may have scared away some potential users of open-source software. Although the dangers of using open-source software are sometimes overstated, every company should carefully monitor what open-source software it has (if any) and how that software is used within the organization. Moreover, any company considering the use of such software should be aware of the legal consequences of that use before either adopting open-source software for internal use or incorporating it into a product for commercial sale. In particular, companies should:

- Perform an intellectual property audit to determine, among other things, just what software is on their systems and under what license arrangements.
- Develop and disseminate internally a written policy regarding the use of open-source software and educate employees about the possible consequences of such use.
- Require the review and approval of any open-source software before it is used internally or as part of the company’s products.
- Ensure that employees and third-party contractors do not incorporate open-source software into any products intended to be proprietary unless the license for the open-source software clearly permits the contemplated use. ■



One Commercial Place, Suite 1800
Norfolk, Virginia 23510

Return Service Requested