

Computer Law News

A Publication of the Minnesota State Bar Association Computer Law Section

Winter 2004-05

Vol. 21, No. 1

Report From the Chair by Katheryn A. Andresen.....	2
2005 Schedule of Events.....	2
Editor's Report by Damien A. Riehl	2
Treasurer's Report by Kari J. Wangenstein.....	3
Committee Reports	3
Case Law Update by Christopher Hilberg.....	6
House Passes Spyware Legislation by Allen J. Oh	7
New Technologies Create New Risks: Traditional CGL Policies May Not Cover Internet Attacks on Your Business by Andrew M. Hansell, Lindquist & Vennum PLLP	9
Computer Law Section Meeting Minutes by Thomas R. Sheran, Secretary	12
Publication Submission Guidelines	16
Computer Law Section New Member/Committee/Officer Interest Form.....	17
2004-05 Computer Law Section Council	18

Damien A. Riehl, *Editor*
651-398-6932
Damien_Riehl@mnd.uscourts.gov



REPORT FROM THE CHAIR

by Katheryn A. Andresen



The Computer Law Section has been an active section in the Minnesota State Bar Association for two decades. Membership, which spiked and decreased in keeping with the rest of the dot.com boom and crash, has kept a strong base membership of close to 200 members. As noted in the survey results in this newsletter, our members are as diverse as the field of technology law: intellectual property (patents, trademarks, copyrights), litigation, IT licensing, contracts, and includes both in-house and firm counsel. We are continuing to participate in local law school events to promote the section to law students.

Our goal is to provide a section that effectively meets the needs of its members, in addition to teaching and inspiring them through noontime CLEs, the Computer Law Institute, and technology roundtable discussions. I would like to extend a welcome to all members to join us at our regularly scheduled meetings held on the second Tuesday of every month. These meetings include a half-hour council business meeting, followed by an hour's presentation on various relevant topics. For the dates and times of the Computer Law Section's meetings, please visit our website at http://www2.mnbar.org/sections/computer_law/. Please feel free to contact me or anyone on the council if you have any comments or suggestions on how we can improve the section to meet your needs.

Happy Holidays and Happy New Year!

2005 SCHEDULE OF EVENTS

Tues., Jan. 11	Section Meeting	11:30 at MSBA Headquarters, City Center
Tues., Feb. 8	Section Meeting	11:30 at MSBA Headquarters, City Center
Tues., Mar. 8	Section Meeting	11:30 at MSBA Headquarters, City Center
Apr. 1	Newsletter Submission Deadline	
Tues., Apr. 12	Section Meeting	11:30 at MSBA Headquarters, City Center
Tues., May 10	Section Meeting	11:30 at MSBA Headquarters, City Center
May (TBA)	Annual Meeting	TBA

EDITOR'S REPORT

by Damien A. Riehl

Every new endeavor provides challenges as well as opportunities for change. In this, my inaugural issue as editor of the *Computer Law News*, I would first like to thank Dianne Plunkett Latham, who has capably steered this newsletter into a positive direction for the past five years. Because of her work, the newsletter has been transformed into an all-electronic medium that is fitting for a section that focuses on computers and technology. Her



fine work is greatly appreciated, and she leaves the Computer Law Section in a better state than when she found it.

You may notice that the format of the newsletter has changed from that in prior years. Because the newsletter has become solely electronic (save for a few members who have not yet provided their e-mail address), these changes to the newsletter have reflected that transition. More color has been incorporated to add interest and to break from the tyranny of the monochrome printing press. We have also changed the font to one that is more easily read on the screen. Further, the use of columns has been greatly reduced to decrease the amount of scrolling necessary to read an entire article. Finally, the newsletter has been changed to a format that can be easily converted to HTML, which will be helpful for those with disabilities, who may use screen readers, or who are otherwise unable to open PDF documents.

I am excited about these changes and believe that they will continue the newsletter's tradition of providing our members with timely, interesting information that is helpful to their practices. If you have any suggestions on how we can improve the newsletter, please send me your comments. I look forward to working with the section and this newsletter's contributors in building on the section's successes.

Newsletter Submissions — Please e-mail any submissions to me at damienriehl@comcast.net. These can include articles, photographs, committee reports, CLE notices, and other information that may interest the members of the Computer Law Section.

TREASURER'S REPORT

by Kari J. Wangenstein

The Computer law Section operates on a fiscal calendar from July 1st to June 30th and continues to be financially sound. The beginning year balance was \$4,891.27 which doubled with this year's membership dues of \$4,984.50. The balance as of October 31, 2004 was \$7,764.89. The Council approved a \$500 budget for the Membership Committee to include the survey recently conducted as well as law student outreaches at the local law schools. The Council also approved at the annual meeting to fund \$625 towards the networking lunch provided during the Computer Law Institute.

COMMITTEE REPORTS

Computer Law Institute

The Annual CLI Committee is responsible for planning and facilitating the annual Computer Law Institute (CLI), which is sponsored by the Computer Law Section. The CLI is a full-day conference featuring speakers and panels on emerging and leading computer law topics and provides participants an opportunity to network with others practicing in this area. The annual CLI is held in the Fall at the Minnesota CLE center, and attendees receive continuing legal education credits. Planning for the annual CLI will begin in early 2005.

This year's Computer Law Institute was held on September 9, 2004. The institute was both successful and well attended with over 125 attendees. The first keynote speaker was the Acting Deputy Assistant Secretary for the Department of Commerce's International Trade Association, Patricia Sefcik, and she spoke on the role of IT and E-commerce in the United

States' economic growth. The lunchtime keynote speaker, Gary Smaby, spoke on the state of venture capital here in Minnesota since the technology crash in 2000. The favorite session of the attendees was the "top ten" panel, which included both technology providers as well as technology end users who gave their top ten things to focus on in a software licensing deal. The Computer Law Institute was structured to allow for a networking lunch period followed by the lunch speaker.

Annual Meeting Committee

The Annual Meeting Committee is responsible for planning the annual Computer Law Section meeting. This meeting is an opportunity for the section to meet and plan for the next year, and the officers for the next year are inducted. In past years, activities have ranged from a group activity to a speaker engagement. The annual meeting is traditionally held in the early Summer, around May. Planning for the annual meeting will begin in early 2005.

Nomination / Bylaws Committee

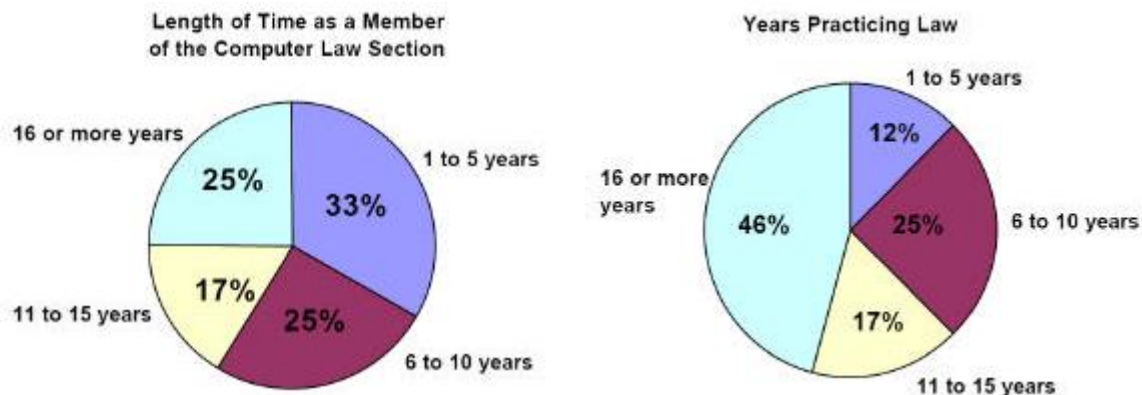
This committee is responsible for nominations for the slate of candidates for delegates and officers of the Computer Law Section. In conjunction with this duty, the committee monitors the Council's activities and procedures to insure compliance with the section's bylaws. The committee also assists the Secretary with parliamentary questions, as well as reviewing and recommending changes to the Bylaws when appropriate.

Legislative Update

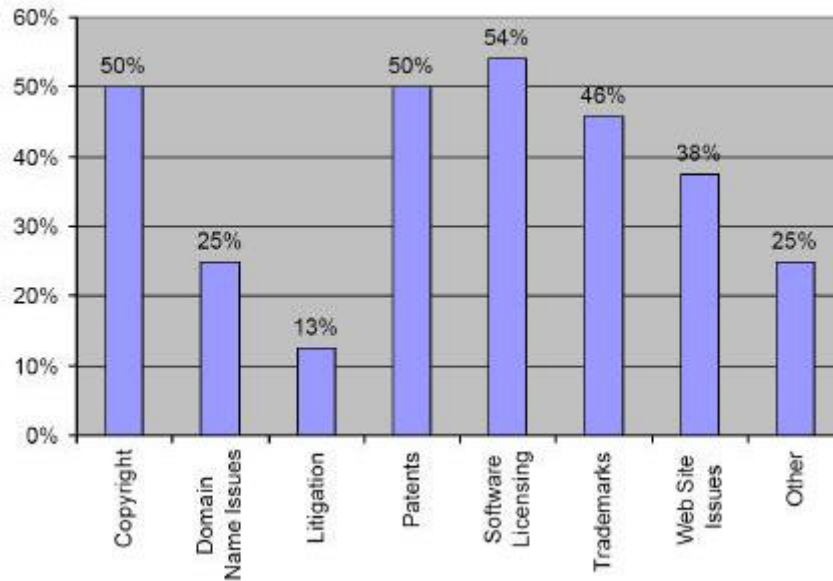
The Legislation Committee considers and reports on legislative activities that are of interest to attorneys who practice computer law. In October 2004, the Committee presented a report on recent anti-spyware legislation that can be found on page 6 of this issue.

Membership Committee & Law Student Outreach

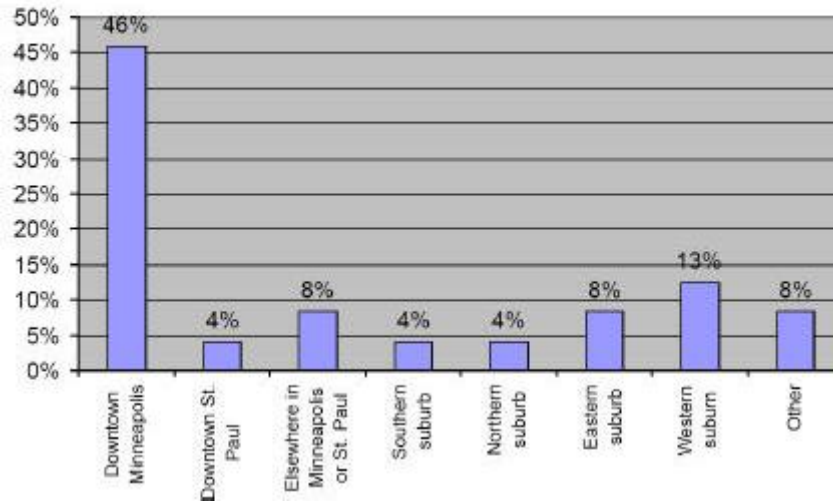
In November, the Membership Committee surveyed the section members to better understand the composition of the section and the needs of the members. Over 10% of the members completed the survey. Some findings are shown below:



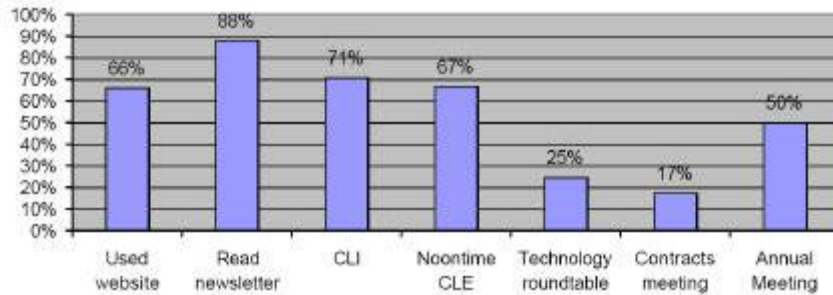
Areas of Law Practiced by Section Members



Location of Members' Offices



Participation in the Section



CASE LAW UPDATE

by Christopher Hilberg

Lexmark v. Static Control Components, **[CA6, 10/26/04] Copyright**

The Sixth Circuit issued a ruling in *Lexmark v. SSC*, vacating the district court's grant of a preliminary injunction against defendant SSC and remanding the case back to the district court for further consideration. Plaintiff Lexmark, a manufacturer of computer printers and toner cartridges, asserted that defendant SSC had violated the Digital Millennium Copyright Act, Section 1201(a)(2), by trafficking in computer chips enabling use of SSC's toner cartridges in Lexmark printers. The Sixth Circuit remanded for consideration of whether Lexmark's authentication code constituted copyrightable expression, and if so, whether Lexmark's "access" mechanisms "effectively" control access by prohibiting other means of accessing its code. The court suggested that Lexmark's access measures do not "effectively" control access, as required under the DMCA for a finding of liability. Accordingly, the decision suggests that Lexmark may not be able to use the DMCA to stop its competitors from creating and selling cartridges that interoperate with its printers: "We should make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case[.]" (conurrence).

The court declined to consider SSC's fair use defense but indicated that there may be a viable fair use defense, depending on the impact of its actions on the market for the authentication code, without regard to the market for toner cartridges. The court noted, "Lexmark has not introduced any evidence showing that an independent market exists for a program as elementary as its Toner Loading Program,



and we doubt at any rate that the SMARTEK chip could have displaced any value in this market."

Eastman Kodak v. Sun Microsystems **[WDNY, 10/1/2004]**

Facing Kodak's request for over \$1 billion in damages, Sun Microsystems settled the patent suit brought by Eastman Kodak, agreeing to license Kodak's patents for \$92 million. Earlier, a jury in Rochester decided that Sun infringed technology belonging to Kodak when it developed and introduced Java more than a decade ago. The US patents—5,226,161; 5,206,951; and 5,421,012—all had a priority dates circa August 1987. The prevalence of Java in existing applications is difficult to overstate. Companies that develop software with Java or use Java-based applications have to wonder, "who's next"? The answer? "Kodak spokesman David Lanzillo declined to comment on whether the company planned to sue others over the patents."

LCW Automotive v. Restivo Enterprises [WDTex, 10/22/04]

A California limousine manufacturer maintained various websites that were accessible in Texas, but they merely provided contact information for potential customers. The websites included a prominently displayed toll-free number or e-mail address and included advertising, but they did not have the capability to process orders or receive funds. The court determined that these websites were insufficient to establish personal jurisdiction in Texas and that merely advertising in at least two nationally distributed magazines was also insufficient to establish personal jurisdiction in Texas.

Mulcahy v. Cheetah Learning, **[CA8, 10/19/2004] Copyright**

Plaintiff Rita Mulcahy is an expert in the field of project management and offers a preparation course and materials to teach students to pass an exam, the Project Management Professional Exam given by the Project Management Institute. Mulcahy sued competitor Cheetah Learning for infringement of her copyrighted book, claiming copyright infringement and unfair competition by Cheetah Learning for distributing allegedly infringing materials to Cheetah students. The District Court granted Mulcahy partial summary judgment and a permanent injunction on her infringement claim.

The Court of Appeals reversed the decision and determined that the district court erred in granting Mulcahy partial summary judgment and injunctive relief on her claim that Cheetah had infringed her copyright on study materials because there were genuine issues of material fact as to: (1) whether Mulcahy's materials infringe on the Institute's exclusive right

to prepare derivative works based on its preexisting copyrighted work and (2) whether Mulcahy's course materials are a fair use of the Institute's work.

"While substantial similarity is the test we use in determining copyright infringement, here the issue is whether Mulcahy's book is a derivative work. In general, the two tests are similar . . . 'Unless sufficient of the pre-existing work is contained in the later work so as to constitute the latter an infringement of the former, the latter by definition is not a derivative work.' . . . It is true that, in most infringement cases, '[i]nfringement of expression occurs only when the total concept and feel of the works in question are substantially similar' . . . But the derivative work issue, like the fair use issue, should turn on 'the qualitative nature of the taking.' . . . Thus, a work may be found to be derivative even if it has 'a different total concept and feel from the original work.'" In a footnote, the court also admonished the district court for enjoining the defendants from reproducing "any materials that are substantially similar" to Mulcahy's work.

HOUSE PASSES SPYWARE LEGISLATION

by Allen J. Oh



A recent EarthLink study found 83 million instances of spyware in a scan of more than 3 million computers between January and September 2004. The typical Internet-connected computer, according to EarthLink, hosts some 26 spyware programs. Chances are that if you surf the Internet, you have downloaded spyware to your computer at some point, perhaps unwittingly.

Spyware can significantly slow the performance of the computers on which they reside. More importantly, spyware can be used to collect personal information about users, such as browsing habits, passwords, and financial information. In an attempt to address the spyware menace, the House of Representatives passed H.R. 2929, the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) on October 5, 2004.

The SPY ACT, if signed into law, would protect computer users by prohibiting a number of practices that are all too common. In particular, the SPY ACT would prohibit deceptive acts or practices that involve any of the following activities:

- using a protected computer to send unsolicited information or material to others;

- diverting a web browser to a website other than the site the user intended to view, without the user's authorization;
- using the computer's Internet connection to cause damage to the computer or to cause the owner or authorized user of the computer to incur unauthorized financial charges;
- using the computer as part of a distributed computing activity that causes damage to another computer;
- delivering ads that the user cannot close without turning off the computer or closing all sessions of the web browser;
- altering certain web browser settings, including the start page, the default Internet service provider (ISP), the bookmarks file, or security settings;
- using a keystroke logger to collect personally identifiable information;
- inducing a user to install software by:
 - presenting the user with an opt-out option but installing the software in spite of the user's opting out,
 - causing a properly uninstalled program to automatically reinstall,
 - misrepresenting that installing a software component or providing login and password information is necessary for security or privacy reasons or to open a particular file type, or
 - inducing a user to install software by misrepresenting the identity or authority of the software provider;
- removing or disabling security, anti-spyware, or anti-virus software; or
- installing or executing software with the intent of causing a person to use the software in a way that violates any of the above prohibitions.

In addition, the SPY ACT would require users to affirmatively consent to installation of software that collects personally identifiable information that it either transmits to another person or uses to deliver ads to the computer. Currently, such "information collection software" can be installed without the user's consent or, indeed, knowledge. Under the SPY ACT, information collection software must display a notice that is clearly distinguishable from other information displayed on the computer. The notice must contain a statement such as, "This program will collect and transmit information about you. Do you accept?" Moreover, the notice must give the user the opportunity to grant or deny consent and must allow the user to cancel installation without granting or denying consent. The notice must also allow the user to see what types of information are collected and the purpose for which the information is collected. The notice must be displayed until the user grants or denies consent, exits installation, or chooses to see what types of information are collected. In addition to the required notice, information collection software must also provide an easily-identifiable way to disable the information collection software and a function that provides that ads delivered by a party other than the software provider are accompanied by an identification of the information collection software.

The SPY ACT would be enforced by the Federal Trade Commission (FTC). For a pattern or practice violation, the FTC may seek a civil penalty of up to \$3M for each

violation of the "prohibited activities" list above, or up to \$1M for each violation of the opt-in requirement. A single activity that violates the SPY ACT with respect to multiple computers would constitute a single violation. On the other hand, a single activity that violates multiple provisions of the SPY ACT (e.g., multiple "prohibited activities") would constitute multiple violations.

Certain activities would not be covered by the SPY ACT. These activities include law enforcement activities and security functions performed by an ISP. In addition, software providers would be allowed to collect information to determine whether a particular user is authorized to use software. The SPY ACT also exempts computer manufacturers or retailers that are merely providing third-party branded software, as well as ISPs that merely provide a connection for information collection software or provide a hyperlink through which a user locates information collection software. Finally, the SPY ACT contains a "Good Samaritan" safe harbor.

The SPY ACT was passed by a 399-1 vote in the House. A similar bill, S. 2145 (the "SPY BLOCK" Act), is pending in the Senate. In November, the SPY BLOCK Act was placed on the Senate Legislative Calendar.

**NEW TECHNOLOGIES CREATE NEW RISKS:
TRADITIONAL CGL POLICIES MAY NOT COVER
INTERNET ATTACKS ON YOUR BUSINESS**
by Andrew M. Hansell, Lindquist & Vennum PLLP

Recent years have seen a virtual explosion of Internet use in the business world. Internet commerce is no longer exclusively used by dot-com companies. Traditional brick-and-mortar businesses have responded with initiatives to allow customers to access accounts, execute transactions, and communicate over the Internet. Even if a business does not complete transactions over the Internet, the connection of its computers to the World Wide Web through e-mail alone may give hackers and viruses a window of opportunity to cause damage. The widespread use of the Internet has created new risks that might not be covered under traditional commercial general liability (CGL) insurance policies. Traditional CGL policies are often triggered only by physical damage to property or individuals and specifically enumerated torts. Because attacks on computer systems often result in no physical damage and are not among the listed torts, a CGL policy may not offer protection for these risks. These new realms of electronic risks may require your business to obtain new insurance coverage.

New Risks In Cyberspace

The rise of the Internet as a tool in the business world has created new risks. Chief among these are attacks by hackers and viruses on business computer systems. Examples of these attacks include so-called denial of service (DOS) attacks, e-mail worms, and unauthorized access to information. These attacks can result in anything from the loss of access to the business's computer system by consumers or employees to the theft or destruction of proprietary and customer information. The consequences of these attacks can be broken into two distinct categories: first-party losses to the business itself and potential liability to third parties.

Examples of potential first-party losses included damages resulting from the business's website or computer system being disrupted or shutdown. As a direct consequence of this

damage, businesses may lose sale transactions and incur other costs from employee and business downtime.

Third-party liability may include actions against a business as a result of the unauthorized access or theft of customers' or clients' personal or proprietary information. In addition to traditional tort actions, concerns over data privacy have resulted in a number of specific laws creating causes of action against a party who discloses private information without authorization.[1]

While these types of claims would likely be covered under a traditional CGL policy if they occurred in the physical world, these claims might not be covered when they occur in the non-tangible world of cyberspace.

Cyberspace Claims May Not Trigger Traditional CGL Policies

A standard CGL policy defines "property damage" as "physical injury to tangible property including the resulting loss of use of that property." However, the corruption or theft of computer data by viruses or hackers seldom causes any actual physical damage to the computer or data storage device. Additionally, courts are split on whether computer data can be considered "tangible" for purposes of a CGL policy.

Court decisions regarding whether computer data is covered by a CGL policy as "tangible property" are far from uniform. For example, in Minnesota, an appellate court concluded that computer data was covered "tangible property" where the tape containing the data was physically lost.[2] A year later, the same court concluded that confidential data was not "tangible property" because the information itself was not tangible and therefore was not covered under a CGL policy.[3] In fact, courts across the country have reached differing conclusions whether data stored on a computer can be considered tangible property.[4]

Similarly, liability actions against a business based on the theft of computer data might also not be covered by a CGL policy. The theft of personal data is not a physical injury to the third party. Standard CGL policies do provide coverage for "violation of the right of privacy" as a personal injury. However the theft of confidential data does not likely fall into any of the traditional causes of action for invasion of privacy.[5]

At the very least, court decisions demonstrate uncertainty about whether a traditional CGL policy will provide coverage from damages incurred as a result of cyberspace attacks. Additionally, in response to these court cases and to policyholders who seek coverage for cyberspace claims under CGL policies, insurers have begun to specifically exclude such risks in the terms of their policies. As a result, businesses should consider whether they should acquire computer-specific policies to insure against these risks.

New Products Offer Coverage – Cyber-Risk Policies

In response to the risks presented by businesses operating on the Internet, some insurers now offer endorsements to their CGL policies that are designed to specifically cover these so-called "cyber-risks." Some insurers have also created completely separate policies to cover these risks.

Uncertainty exists in the underwriting of these new cyber-risk policies because insurers lack sufficient actuarial information or loss histories. As a result, there is little uniformity in the type or terms of coverage in these policies and the coverage offered is often limited in scope. Some common limitations on cyber-risk policies include:

- **"Claims made" coverage** – Most cyber-risk policies are offered on a "claims made" basis rather than an "occurrence" basis. The coverage will apply only to claims made against the insured during the term of the policy. The policy will not cover claims

made against the insured after the term of the policy, even if the incident occurred during the policy's term.

- **Limited to either first-party or third-party coverage** – Many cyber-risk policies will cover either direct losses of the insured (such as business interruption and loss-of-use damages) or liabilities to a third-party (such as claims for stolen customer information), but not both.
- **Insiders' Exclusion** – Most cyber-risk policies will contain a provision excluding losses caused as a result of dishonest acts of an employee of the insured.

As part of the underwriting process, most cyber-risk policies require the inspection and approval of the covered computer system by a technical expert. An independent expert often conducts this inspection. The policy may also require a continuing periodic inspection and certification of the insured's system to assure adequate security measures are continually updated as a condition of coverage.

Businesses should bear in mind that the interpretation of the new cyber-risk policies by the courts remains an open question. Because cyber-risk policies contain many new terms and cover areas that have not been previously addressed in insurance policies, the interpretation of these terms and coverages by a court is not well settled. Accordingly, the actual scope of coverage afforded under these policies is not well defined.

The widespread use of the Internet in business has opened the door to new opportunities and new risks in the non-physical world of cyberspace. Businesses must be aware of these evolving and emerging risks and adapt accordingly. Given the increasing use of the Internet by businesses, it seems likely that cyber-risk coverage will become part of any business's risk management plan.

Notes

[1] Examples of laws creating causes of action for individuals based on the disclosure of information include: portions of the Gramm-Leach-Bliley Act (GLBA) (regulating financial institutions); the Health Insurance Portability and Accountability Act (HIPPA) (regulating health care providers); and the Children's Online Privacy Protection Act (COPPA) (regulating the collection of data from children).

[2] See *Retail Sys., Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735 (Minn. Ct. App. 1991).

[3] See *St. Paul Fire & Marine Ins. Co. v. Nat'l Computer Sys., Inc.*, 490 N.W.2d 626 (Minn. Ct. App. 1992).

[4] See *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 466 (E.D. Va. 2002) (collecting cases).

[5] The tort of invasion of privacy includes four general categories: (1) intentional intrusion into the private affairs of another; (2) appropriation of the name or likeness of another for commercial use; (3) publicizing of private facts; and (4) publicity of another in a "false light."



Andrew M. Hansell advises clients on commercial litigation, products liability, public law, and insurance coverage. He can be contacted at 612-371-3204 or at ahansell@lindquist.com.

This article, originally published in RiskVue in March 2004, is only a general summary for informational purposes and does not constitute legal advice.

COMPUTER LAW SECTION MEETING MINUTES

by Thomas R. Sheran, Secretary

Minutes from September 14, 2004

Attendees: Katheryn A. Andresen (Chair); Kari J. Wangensteen (Treasurer); Christopher J. Schulte (Past Chair); James A. Blomquist; Jenny C. Salyers; Christopher Hilberg; Carolyn M. Sandberg; Stephen W. Buckingham; Charles A. Johnson; Steven C. Lieske; John P. Sumner; Carla Condiff Schaumann; Allen Oh; Lisa Wilde

Call to Order. The Chair called the meeting to order at 11:40 a.m.

Minutes. There were no prior minutes to approve.

Treasurer's Report. None.

Committee Reports:

Newsletter. None.

Noontime CLE. None.

Contracts. None.

Case Law. None.

Law Student Outreach. None.

Website Committee. Chris S. reported that the website has been updated to include this year's meeting dates..

Computer Law Institute. Kate A. reported that 110 registrations have been received so far for this year's CLI

Legislation. None.

Elections Committee. None.

Annual Meeting. None.

Old Business. No old business.

New Business. The Chair indicated that she received membership numbers for the past five years which showed a high of 351 members in 2000 and a low of 272 in 2003. The Chair invited comments on setting goals for more members and more CLE hours. The Council discussed the merits of setting such goals. After discussion Steve B. moved to form a membership committee to look into the issue. The motion was seconded by Jim B. and approved by the Council.

The Chair also discussed format for the monthly meetings. Steve B. moved that the chair assign a committee to be responsible for noon-

time presentations to be held at 11:30 before the Regular Meetings. John P. seconded the motion and the Council approved it. Jen S. agreed to handle the topic for the next meeting in October before the business portion of the meeting.

The Chair then asked those interested in serving as chair of a committee to let her know and she would make the assignments in the near future.

Lisa Wilde introduced herself as the Section's new MSBA liason.

Chris H. moved the meeting be adjourned, Steve B. seconded, and the Council voted to adjourn. The meeting was adjourned at 12:45 p.m.

Christopher Schulte, Acting Secretary

Minutes from October 12, 2004

Attendees: Katheryn A. Andresen (Chair); Christine M. Brick (Vice Chair); Thomas R. Sheran (Secretary); Kari J. Wangensteen (Treasurer); Christopher J. Schulte (Past Chair); Miguel Azar; James A. Blomquist; Barbara Grahn; Jenny C. Salyers; Charles P. Brink; Christopher Hilberg; Carolyn M. Sandberg; Stephen W. Buckingham; Charles A. Johnson; Colleen M. Schmid (by phone); Carla Condiff Schaumann; John A. Taft; Frank S. Farrell, Jr.; Daniel A. Tysver; Gary S. Weinstein; Allen Oh; Lisa Wilde

Call to Order. The Chair called the meeting to order at 11:40 a.m.

Minutes. Prior minutes approved.

Treasurer's Report. Financial report for period ending August 30, 2004. Kari Wangensteen reviewed charges for the Computer Law Institute. \$1000 had been budgeted but charges were less than projected and with reduced charge for notices to the Business Law Section the total charges were about \$600.

Committee Chairs. Kate Andresen reported that the following persons have agreed to serve as this year's committee chairs:

Committee	Chairperson
Newsletter	Damien Riehl
Noontime CLE	Jen Salyers
Contracts	
Website Committee	Chris Schulte
Computer Law Institute	Christine Brick
Legislation	Allen Oh
Case Law	Chris Hilberg
Membership & Law Student Outreach	Steven Lieske Steve Buckingham Kari Wangensteen
Annual Meeting	Christine Brick

Committee	Chairperson
Bylaws / Elections Committee	Chip Brink
Tech. Roundtable	Gary Weinstein

Committee Reports:

- Newsletter.** Kate Andresen reported that Damien Riehl had agreed to serve as Newsletter committee chair. No decision has been made about the format for future newsletter but Kate will check with Damien to get his input.
- Noontime CLE.** Jenny Salyers reported that she is planning to check with Allen Oh regarding time slots for future noontime CLE presentations. The current plan is to have a speaker at each meeting.
- Contracts.** No report.
- Case Law.** Chris Hilberg will present a report on recent case law at the November council meeting.
- Law Student Outreach.** Steve Buckingham reported that William Mitchell is having a career day at which the Intellectual Property Law Institute is expected to have a table. Kate Andresen and Charlie Johnson agreed to represent the Computer Law Section at the career day. Steve Buckingham will check with William Mitchell regarding the mechanics of getting a table.
- Website Committee.** Council members were encouraged council members to check the website and submit suggestions about updates and improvements. Kate Andresen discussed a possible integration of Newsletter and Website committees.
- Computer Law Institute.** No report.
- Legislation.** After the meeting, Allen Oh made a presentation of information regarding Spyware legislation.
- Elections Committee.** No report.
- Annual Meeting.** No report.
- Old Business.** No old business.
- New Business.** **Roundtable Discussion Programs:** A discussion was had regarding last year's experience with three technology roundtable programs drawing 10 to 30 participants. Kate Andresen suggested that future roundtables be scheduled to take place after the regularly scheduled council meetings. This arrangement would leave 2 available dates. Gary Weinstein agreed to chair the committee and will coordinate with the noontime CLE committee to schedule programs after the council meetings. It was suggested that the scheduled dates for noontime CLE and roundtables be posted on the Section website.
- Membership Survey:** Steve Buckingham reported on a plan to determine the level of membership interest in existing and/or new section services. Proposed survey questions have been drafted. Suggestions regarding additional survey questions should be submitted

to Steve Buckingham or Steve Lieske. Steve Buckingham reported that Survey Monkey offers a survey handling service for about \$40.

Kate Andresen proposed a budget for the New Member committee of \$500 to include the conduct of the proposed member survey and the student outreach program. A motion to approve the \$500 budget was passed.

MSBA Legislative Committee: Kate Andresen reported that the MSBA had inquired about a Computer Law section representative to serve on the MSBA legislative committee. A legislative committee meeting is scheduled for 12/03/04 to prepare for the legislative session that begins 1/4/05. A position on the committee is open to volunteers.

Motion to Adjourn.

The meeting was adjourned at 12:05 p.m.

Thomas R. Sheran, Secretary

Calling All Addresses!

If you received a hard copy of this issue instead of a copy via the Internet, it means that the MSBA does not have your e-mail address. Less than 3% of our members still receive this newsletter via the quaint "snail mail" method. Don't be left behind! Newsletters sent via e-mail arrive one to two weeks earlier than those sent via surface mail.

We value your inbox privacy. We promise that we will not provide your e-mail address to any third party.

Please submit your e-mail address to 612-333-4927 or mkempton@statebar.gen.mn.us.

PUBLICATION SUBMISSION GUIDELINES

The Computer Law Section welcomes submissions for publication in this newsletter. If you submit an article, please adhere to the following guidelines:

Subject Matter. – Submit any articles of interest to the members of the Computer Law Section, including recent issues on technology licensing, patents, copyright, trademark, or Internet technology. Articles previously published in other publications are acceptable, if current. Preference is given to local authors.

Article Length – Articles should preferably be 3,500 words or less, but not more than 5,000 words, as the length of the newsletter is limited.

Article Format – A journalistic style is preferred over the style of law reviews, CLE materials, or legal briefs. The structure of the article should consist of a “catchy” lead, a “thesis paragraph” tersely stating the general theme of the article, an exposition of the topic, and a summary conclusion.

Footnotes – Keep law-review-style footnotes to a minimum, as this is a journalistic publication. All footnotes should be in the form prescribed by the Uniform System of Citations (“Bluebook”). Footnotes should be limited to citing specific authorities; “string” citations and discursive notes are discouraged. The author is responsible for ensuring the completeness and accuracy of all references and citations, as article information and footnotes are not checked for accuracy.

Copyright Notice – A Copyright notice is unnecessary. If the author wishes to include

one, it should be placed at the end of the article, not on each page.

Title and By-Line – The article should include both a title and a by-line. The by-line should include both the author’s name and firm affiliation. It is not necessary to include any additional author biographical information. Keep the author’s practice areas, experience, etc., to a minimum.

Photographs – Photographs of article authors and Section events are encouraged. Digital photographs are preferred, although prints are also acceptable.

Graphs and Charts – The use of graphs and charts should be kept to a minimum.

Submission Deadline – The *Computer Law News* is published twice a year: in December and in May. Submission deadlines are approximately 4 weeks prior to publication and are listed in the Calendar of Events for the prior issue. Microsoft Word files sent via e-mail are preferred, though other formats are permissible.

Distribution – The newsletter is distributed via e-mail and is also posted on the Computer Law Section’s website. Those section members who have not submitted an e-mail address are sent a hard copy via U.S. mail.

Questions – Contact Editor Damien A. Riehl, at: 651-398-6932 or damienriehl@comcast.net

COMPUTER LAW SECTION NEW MEMBER/COMMITTEE/OFFICER INTEREST FORM

- Q** Enclosed is my check in the amount of \$35 payable to the MSBA.
(Mail to Section Services, c/o MSBA, 600 Nicollet Mall, Suite 380, Minneapolis, MN 55402.)
- Q** I am a current Computer Law Section member. The following information is address change information only. Address information can be faxed to 612-333-4927; or e-mailed to mkempton@statebar.gen.mn.us.

Name _____

Employer _____

Street _____

City/State/Zip _____

Phone _____ Fax _____

E-mail _____

If you are interested in joining one of the following committees for 2003-2004, or are willing to be considered for an officer or committee chair, please check below and send to Computer Law Section Chair.

	Chair	Join
Annual Meeting	_____	_____
Computer Law Institute	_____	_____
Case Law Reports	_____	_____
Contracts	_____	_____
Law School Outreach	_____	_____
Newsletter Editor	_____	_____
Noontime CLE Programs	_____	_____
Legislative Liaison	_____	_____

I would like to participate in the Section in the following ways:

Speak at a CLE Contribute an article to the Newsletter

Other: _____

Check any of the following officer positions you would consider in the future:

Chair Vice Chair Secretary Treasurer Council member

I would like to see the Computer Law Section undertake the following:

2004-05 COMPUTER LAW SECTION COUNCIL

Section Council

Katheryn A. Andresen

2004-05 Chair

Minneapolis

(612) 341-3000 kandresen@bssdlaw.com

Christine M. Brick

Vice-Chair

2005 Computer Law Institute Chair

Annual Meeting Committee Chair

Minneapolis

(612) 316-0939 Christine.Brick@wellsfargo.com

Kari J. Wangenstein

Treasurer

Membership & Law Student Outreach Co-Chair

Minneapolis

(612) 291-7437 kari.wangenstein@bestbuy.com

Thomas R. Sheran

Secretary

Minneapolis

(612) 347-0300 sherant@moss-barnett.com

Christopher J. Schulte

2003-04 Chair

Website Committee Chair

Minneapolis

(612) 371-1314 cschulte@meagher.com

Damien A. Riehl

Newsletter Editor

Minneapolis

(612) 664-5072 Damien_Riehl@mnd.uscourts.gov

Council Delegates for 2004-05

Miguel J. Azar

Minneapolis

(612) 701-8471 mazar@minn.net

James A. Blomquist

Minneapolis

(612) 373-8559 jblomquist@felhaber.com

Charles P. Brink

Bylaws / Elections Committee Chair

Minneapolis

(612) 344-0600 chip@brinklaw.com

Stephen W. Buckingham

Membership & Law Student Outreach Co-Chair

St. Paul

(651) 733-3379 swbuckingham@mmm.com

John J. Carney

St. Paul

(651) 695-1757 jjc@alum.mit.edu

Carla Condiff Schaumann

Minneapolis

(612) 869-6805 ccschaumann@mn.rr.com

Frank S. Farrell, Jr.

Minneapolis

(612) 373-6908 ffarrell@slwk.com

Michelle Gilbertson

Law Student Outreach Co-Chair

Minneapolis

(612) 667-0434 Michelle.Gilbertson@wellsfargo.com

Barbara J. Grahn

Minneapolis

(612) 607-7325 BGrahn@Oppenheimer.com

Christopher R. Hillberg

Case Law Chair

Minneapolis

(612) 607-7386 chilberg@oppenheimer.com

Charles A. Johnson

St. Paul

(651) 635-7702 c.a.johnson@unisys.com

Steven C. Lieske

Membership & Law Student Outreach Co-Chair

Minneapolis

(612) 607-7508 slieske@oppenheimer.com

Ronald P. Marmo

Minneapolis

(612) 245-9013 Ronmarmo@juno.com

Allen Oh

Legislation Committee Chair

Minneapolis

(612) 332-8200 ajoh@mhsiplaw.com

Kendra L. Rubbright Richgels

Minneapolis

(612) 316-1446 Kendra.Richgels@wellsfargo.com

Jenny C. Salyers

Noontime CLE Chair

Minneapolis

(612) 341-3005 jsalyers@bssdlaw.com

Carolyn M. Sandberg

Minneapolis

(612) 371-3929 csandberg@lindquist.com

Colleen M. Schmid

Minnetonka

(952) 936-1861 colleen_m_schmid@uhc.com

Sandra M. Sedo

Minneapolis

(612) 340-8746 sedo.sandra@dorsey.com

John P. Sumner

Minneapolis

(612) 332-8200 JPSumner@mhsiplaw.com

John A. Taft

St. Paul

(651) 733-1750 jataft@mmm.com

Daniel A. Tysver

Minneapolis

(612) 915-9634 dtysver@bitlaw.com

Gary S. Weinstein

Technology Law Roundtable Committee Chair

Minneapolis

(612) 766-8309 gweinstein@faegre.com

PRSR STD
U.S. Postage
Paid
Mailed From
Zip Code 55101
Permit NO. 6885