Message from the Chair

The clouds parted and the sun came out on our final day in Los Angeles for the Cyberspace Law Committee's 2013 Institute on the Law of Cyberspace. I was able to take in some of my old haunts around Westwood (Falafel King! Coffee Bean! Same as back in UCLAW days) before heading back to SF, and I hope our Minnesotan and East Coast colleagues enjoyed the brief respite from those single-digit weather zones.

MEETING RECAP

For those who missed the meeting, here's a recap of our substantive sessions, with my take on some of the takeaways:

CLE Sessions

- **BIG DATA - NEW PRIVACY ISSUES FROM NEW SERVICES BASED ON DATA FROM ELSEWHERE.** We kicked off the CLE with a presentation from John Pavolotsky of Greenberg Traurig in San Francisco on the emerging big data analytics business models and how big data-related privacy issues have been treated by courts so far, or might be treated by courts by analogizing to the emerging geolocation privacy cases. He also spoke about what we might see next, as courts start to address the complex privacy and other issues that are emerging from the new ways businesses are offering services based on data generated about others. … certainly more will come soon in this area. A copy of John’s slides is [here](#).

- **ONLINE CONTRACT FORMATION - CONTRACTS v. NOTICES - LAW** professor Nancy Kim, from the California Western School of Law in San Diego, joined us next, to offer some of her challenging view of how courts are getting it wrong when they analyze website terms of use under standard contract formation theories. Nancy presented her ideas about considering the idea of a notice rather than a contract, when considering how the terms of use should be enforced. Nancy’s work in this area picks up on the detailed and rich history within the Cyberspace Committee in analyzing contract formation in cyberspace (see the committee’s well-cited series of articles from The Business Lawyer on click-throughs, click-wraps, browse-wraps, and similar agreements, and their modifications). There seems to be as much interest as ever in how courts are analyzing terms of service and terms of use, and how their provisions should be enforced. Nancy's slides are [here](#); contact Nancy for any updates.

- **CONTENT LICENSING IN THE ENTERTAINMENT INDUSTRY - HOW DIGITAL DISTRIBUTION MODELS HAVE BEEN STYMIED AND MIGHT EVENTUALLY FLOURISH.** LA-based practitioner and adjunct professor at the Southwestern Law School, Louise Nemschoff, presented a very useful primer on the convoluted background of the ways content owners license music and film content, including some helpful summaries of the principal rights administration/licensing agencies that operate in this sphere. Louise’s presentation provided some insight into the impediments to widescale expansion of digital distribution systems, as well as some views about what lawyers might need to monitor as technology clients seek to grow content-related businesses. Louise’s slides are [here](#); contact Louise for any updates.

- **LEGAL DUTIES ARISING FROM CYBERATTACKS ON THE GRID.** Longtime committee contributor Roland Trope, despite being under strict doctor's orders to stay home and recuperate from pneumonia, joined via teleconferencing with fellow New Yorker and technology lawyer Steve Humes of Holland & Knight (Steve was actually present...
Governments Control the Internet

Cyberlaw Gigs

Your Articles Are Welcome

Newsletter Editors:
Cheryl Dancey Balough
cbalough@balough.com

Lois Mermelstein
lois@loismermelstein.com

in the room) to give as up-to-date and frightening a view as ever of the legal duties that are arising from cyberattacks on the electrical grid. Roland and Steve gave some useful background for us non-utility lawyers on how the US grid is set up and managed, and they offered some valuable insight on how increasing cyberattacks are creating board issues and duties to understand cybersecurity risks and implement and update cybersecurity protection measures.

Contact Roland for more info or copies of materials.

- THE DAY THE CARS STOOD STILL: 1951 SCI-FI OR 2013 REALITY? Cheryl and Richard Balough of the Balough Law Offices in Chicago gave a thoroughly entertaining and insightful presentation on how the increasing world of cyberhacking is penetrating beyond our offices and homes and into our cars. We may soon see the day when hacker malware will stop us dead in our tracks as we try to make it from home to the grocery store. See Cheryl and Richard's presentation for a closer view of how intimately all our vehicles are now controlled by, and controllable through, the Internet. You may access the Baloughs' slides here.

- DIGITAL LAW 2013: HOT TRENDS AND ISSUES IN CLOUD, MOBILE AND INTERNET LAW AND LIABILITY. Longtime Cyberspace Committee contributor and Internet Law Treatise author Ian Ballon, of Greenberg Traurig in LA & Palo Alto, gave a whirlwind tour of the latest developments in internet litigation, with practical and insightful comments, as always, on the new ways litigation strategies are playing out in courts around the country. Contact Ian for a copy of the slides, including the most up-to-date citations for recent decisions and comments on current strategy in cases involving everything from the DMCA and Section 230 to class action privacy claims and more.

- STRATEGIC REMEDIES FOR CYBERCRIME VICTIMS - Mark Mermelstein, of Orrick in Los Angeles, joined us to offer some up-to-date reports on criminal prosecutions involving a variety of cyberlaw matters. Mark's presentation offered a strategic way of thinking about referrals to prosecutors - whether the US attorney's office, local law enforcement, or a state AG office - when a client's digital property has been stolen or another type of cybercrime has occurred. Mark's presentation linked nicely to our new project to address the increasing criminalization of technology and IP disputes, and we will certainly see more in this area. A copy of Mark's slides is here.

Provocative Lunch Keynotes

As we did last year, we invited two local lawyers to address us at lunch. First, studio lawyer, and former Yahoo lawyer, Melinda Demsky of Fox gave us some comments - with fun pictures and clips - on the studio view of the continued proliferation of online piracy. As expected, the studios seem to think piracy is as much of a problem as ever, and this presentation reminded us, at least, that there are a host of actors out there in cyberspace who are making a buck on the studios' dime.

Next, we were fortunate that Dean Erwin Chemerinsky, founding dean of the UC Irvine School of Law and longtime contributor to many bar publications and programs, was able to survive the horrendous rainy-day traffic from Orange County just in time to give us a positively captivating talk about the ways that First Amendment jurisprudence - specifically that focused on defamation and privacy law - is changing and may need to change further as a result of the evolving ways that speech is disseminated on the internet.

Thanks to both our lunch speakers for providing further provocative content for our group.

Breakouts and Roundtables

Our CLE Institute was followed by a series of moderated roundtables and breakout sessions devoted to our subcommittees and task forces, as well as specific ongoing or new projects of the committee. Some of those topics and projects include, along with committee leaders to contact if you want more information, follow. More in-depth summaries of the discussions are provided in the February newsletter.

- Cybersecurity & the Grid. Counsel's guide - Roland Trope.
• *Wait! Now I Need to Learn IT Too?* Discussion and projects related to the amendments to the ABA model rules of professional conduct - Juliet Morigiello and Lois Mermelstein, Task Force on Professional Responsibility & Technology.

• *Privacy and Surveillance in the Digital Age.* A discussion of pending and potential legislative developments involving privacy and security - roundtable conducted by Prof. Jack Lerner of the USC Gould School of Law. If you were not at the roundtable and are interested in participating in a project involving tracking legislative developments related to privacy, please contact Jon Rubens.

• *Bringing your Mobile Device to Work.* Discussion and project on BYOD policies - eCommerce Subcommittee - Ted Claypoole & Richard Balough.

• *ULC Drafting Committee Project on Digital Death Issues.* Prof Christina Kunz, Wm. Mitchell School of Law updated the group on her work as official liaison of the Business Law Section to a Uniform Law Commission drafting committee addressing issues surrounding digital asset ownership, including transition of ownership to digital assets at death.

• *Criminalization of Technology Task Force.* Cathy Gellis and Jamie Clark led this discussion of a possible new project or task force of the committee, focusing on the emerging issues and growing concerns surrounding the increases in criminalization of disputes involving technology and online IP.

• *Consumer Subcommittee.* Ongoing work on updating safeshopping.org, safeborrowing.org, and potentially safeselling.org - see subcommittee chairs Profs. Jim Nehf, University of Indiana, Indianapolis School of Law, and John Rothchild, Wayne State University School of Law.

• *Subcommittee on International Trade.* Several projects and matters under review, including potential work on online dispute resolution, ongoing matters at UNCTRAL, and more - see co-chairs Hal Burman and John Gregory for access to materials posted online.

• *Electronic Financial Services Subcommittee.* Prof. Ed Morse and Steve Middlebrook discussed several potential projects for this subcommittee to undertake and reviewed plans for an upcoming program on mobile payments at the Spring Meeting in DC and discussions and presentations planned for Spring and for Annual Meeting in SF.

• *Digital Media Subcommittee.* Prof. Jon Garon of the Chase Law School at Northern Kentucky University engaged the group in a discussion of several ongoing and potential projects involving digital publishing and app development for media and entertainment.

• *Cybersecurity and the Cloud Project.* Contact projects leaders Lisa Lifshitz and Ariane Siegel for more info about the ongoing cybersecurity-in-the-cloud checklist project, as well as updates on plans for a possible program later this year on cloud providers and security issues.

• *Corporate Director Toolkit Project.* We are contributing new chapters to the next edition of this well-selling ABA publication - see project liaison Sarah Jane Hughes.

• *Cloud & IT Services Subcommittee.* Cloud services checklist project and additional potential written projects - see subcommittee co-chairs Phillip Schmandt and Bill Denny for more info.

---

**Thanks to Our Sponsors**

**PLATINUM SPONSOR - BOX**

Big thanks go out to our platinum sponsor Box.com, which made its services available to our committee leadership and to all meeting attendees. And thanks, and welcome, to Box General Counsel Pete McGoff, who attended the meeting and has joined the committee. Thanks also to Julie O'Brien of Box, who attended the meeting and helped many of us configure folders and get others up and running on the service.

For those who wish to access any of the specific content related to breakouts, roundtables, and ongoing committee projects, let us know. We
will put you directly in touch with subcommittee and task force chairs, who then can invite you to access the materials that have been posted to Box.

THANKS TO KIVU, TOO!

Our gold sponsor was Kivu Consulting, whose founder and CEO Winston Krone is a committee member and was in attendance. Thanks for your support Winston and Kivu!

Upcoming Committee Events and More News

We have lots coming up at the Business Law Section's Spring meeting in Washington DC - more below - and we will soon be working on plans for the committee's meetings at the Annual Meeting in San Francisco in August 2013.

Meanwhile, look to our newsletter each month for additional news on the committee, cyberlaw developments gathered by our contributors and committee members, and more reports on our projects, programs, and publications.

Jonathan T. Rubens  
Chair, Cyberspace Law Committee, Business Law Section  
Jon@irlegalgroup.com

Upcoming CLCC Programs

ABA Business Law Section Spring Meeting - April 4-6, 2013

The 2013 Business Law Section Spring Meeting will be held in Washington, DC, on April 4-6. Early bird, discounted registration has been extended till February 15. Here's the schedule for the Cyberspace Law Committee meetings, and CLE programs we are presenting or co-sponsoring.

Thursday, April 4, 2013

- 8am - 10am: Program: What Your Payments are Telling People: Privacy and the Mobile Payment Race
- 9am - 10am: Main Cyberspace Law Committee Meeting
- 11am - 12pm: Cybersecurity Subcommittee
- 11am - 12pm: Cyberspace Task Force on Internet Governance
- 1pm - 2pm: Cloud & IT Services Subcommittee
- 2pm - 3pm: Consumer Protection Subcommittee
- 3pm - 4pm: International Trade Subcommittee
- 4pm - 5pm: Cyberspace Task Force on Professional Responsibility & Technology
- 7:30pm - 10:30pm: Cyberspace Law Committee Dinner

Friday, April 5, 2013

- 8am - 10am: Program: You Win! Or Did Your Client Just Lose?: The Law of Contests
- 8am - 10am: Program: You Sent Funds Where? How to Help Remittance Transfer and Mobile Payments Clients Fess Up When They Mess Up BSA and OFAC Compliance
- 10am - 11am: Financial Services & Payments Subcommittee
- 10:30am - 12:30pm: Program: Legal Ethics and the Law of Lawyering: Where We Are After Ethics 20/20 and Where We Need To Be
- 1pm - 2pm: Marketing and Advertising Subcommittee
- 1pm - 2pm: mCommerce Subcommittee
- 2:30pm - 4:30pm: Program: iPads at the Firewall! Should You Permit Employee Devices into Your Network?
- 4:30pm - 5:30pm: Cyberspace Committee Meeting of Subcommittee and Task Force Chairs

Saturday, April 6, 2013:
10:30am - 12:30pm: Program: Licensed Today, Infringement Tomorrow?: The Termination Right Under the Copyright Act and Other Oddities

There are several other fast-approaching deadlines:

- Advance registration ends on March 12, 2013 (thereafter your name will not appear on the attendee roster)
- No cancellation refunds after March 12, 2013
- Lunch and event tickets do sell out; register early to ensure your spot.

Cyberspace Committee Dinner info and link to purchase tickets is coming soon.

More information about the programming and registration are available [here](#). We look forward to seeing you in DC.

### Other Programs of Interest


The annual [NKU Chase Law + Informatics Symposium](#) will be held on February 15, 2013. The symposium will focus on issues in labor and employment related to informatics, including such topics as social media in the employment context, candidate screening practices, employee privacy, data security and appropriate policies, National Labor Relations Board actions, and proposed legislation to protect employee account access. The program will include a day-long seminar and networking reception. Presentations delivered at the conference will be published by the [Northern Kentucky Law Review](#). A podcast option is also available. [Register here](#).

#### RSA Conference ◆ February 25 - March 1, 2013

The [RSA Conference 2013](#) in San Francisco on February 25 - March 1 offers the theme "Security in Knowledge: Mastering Data, Securing the World." The conference will include a panel on "Do We Have the Authority? Legal Issues in Protecting Government Networks." Two of the panel's speakers are members of the Cyberspace Law Committee: Roland Trope, Partner at Trope and Schramm LLP and Adjunct Professor in the Department of Law, United States Military Academy at West Point, and John Gregory, General Counsel, Ministry of the Attorney General of Ontario, Canada.

#### ABA Intellectual Property Law Conference - April 3-5, 2013

The ABA's 28th Annual Intellectual Property Law Conference, April 3-5, 2013 in Arlington, Virginia offers a wide variety of intellectual property programming, including a workshop titled: "Trademark & Copyright: Dear Congress, Do No Harm to the Internet: An Update on Anti-Piracy and AntiCounterfeiting Legislative Efforts." More details are [here](#).

#### How to Limit Cyber Security Risks and Respond to Cyber Security Breaches

February 11, 2013  
Location: N/A  
Format: Webinar/Teleconference  
[Free for ABA members](#)

#### Social Media Marketing Series #5: Sweepstakes, Contest, & UGC Promotions

February 11, 2013  
Location: N/A  
Format: Webinar/Teleconference

#### The Picasso Problem: Copyright and the Google Art Project

February 19, 2013  
Location: N/A  
Format: Webinar/Teleconference

#### Information Security, Privacy, and the GAO: Perspectives on Risks, Requirements, and Emerging Issues in the Public Sector

February 20, 2013  
Location: N/A  
Format: Webinar/Teleconference
CLCC Publications

Cyberspace Law Survey

The Cyberspace Law Committee is proud to make its Survey of Developments in Cyberspace Law for 2011-2012 available. The efforts of more than a dozen authors, editors, and law student proofreaders and cite checkers make this Survey a high-quality publication that the committee is pleased to feature. Authoring a segment of the Survey is a great way to get involved with the Committee, even if you are unable to participate in meetings or other in-person events. If you're interested in contributing to the next edition, please contact Kristine Dorrain. We will be soliciting authors in the next couple of months.

CLCC Projects

Corporate Directors Tool Kit
Sarah Jane Hughes, University Scholar and Fellow at Maurer School of Law, Indiana University

The committee is joining the contributors to the Corporate Directors Tool Kit project, which produces a book that is now in its 7th edition. The general editors have asked us to identify contributors for four key areas, and possibly a fifth. They are (1) data privacy - particularly outside the US; (2) cybersecurity - particularly after the SEC's Corp. Fin. Division 2011 "guidance" on disclosures; (3) technology licensing; and (4) safe selling online. The fifth topic under consideration includes compliance with regulations enforced by OFAC, FinCEN, and the IRS on anti-money laundering, anti-terrorism, and limitations on transactions with designated states or individuals on federal watch lists.

Drafts will be due to the general editors on July 1, 2013, which means slightly earlier to committee leadership. More than one contributor is likely to be needed for the four primary topics listed above, and we can use reviewers as well. If you are interested and have not already identified your interest, please alert Sarah Jane Hughes and she will send you an invitation to the Box.com area we are creating for this project.

Digital Death Project
Christina Kunz, Professor at William Mitchell College of Law

One of the breakout sessions at the Committee's recent Winter Working Meeting was on the "digital death" project: how executors, conservators, POAs, and trustees ("fiduciaries") of deceased and incompetent persons can gain access to the digital accounts and assets of those persons. Initially presented at last year's Winter Working Meeting, this topic is now the subject of a drafting committee within the Uniform Law Commissioners. Prof. Christina Kunz is an ABA Advisor to the drafting committee, and she convened a WWM brainstorming session on how to draft the act so that it doesn't lead to violations of the federal Stored Communications Act and the Computer Fraud and Abuse Act. The consensus of the group favored treating the fiduciary as having identical access rights as the deceased or incompetent person, rather than implying or interpreting a contract provision to allow such access by the fiduciary as a separate person. Prof. Kunz will forward the thoughts from the brainstorming session to the drafting committee and will update the group on future developments.

The Professional Responsibility and Technology Task Force Needs Your Help!
Co-Chairs Juliet Moringiello and Lois Mermelstein

The Professional Responsibility and Technology Task Force of the Cyberspace Law Committee held two roundtable discussions at the Winter Working Meeting in Los Angeles. We discussed how to best fulfill our charge, which is to guide business lawyers in complying with the technology-related standards that the ABA added to the Model Rules of Professional Conduct in the summer of 2012.

http://apps.americanbar.org/buslaw/committees/CL320000pub/newsletter/201302/
One of the changes to the MRPC is an amendment to the comment to Model Rule 1.1, regarding lawyer competence. Rule 1.1 states that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." The Comment to Rule 1.1 now states that "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

Another technology-related amendment relates to confidentiality of information. Model Rule 1.6 (c) requires lawyers to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 to Rule 1.6 elaborates on the meaning of "reasonable efforts" by stating, in part, that "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."

At our roundtables we agreed to develop a "Business Lawyer's Guide to Assessing the Technologies Used in Law Practice" in order to help lawyers spot the issues involved in using technology in practice. In this guide, we intend to classify technologies according to the functions that they perform in a law practice (such as communications, file storage, and creating and collaborating on documents) and identify the benefits and risks inherent in using technology to perform these functions. By doing so, our goal is to assist lawyers in evaluating new technologies in light of their ethical obligations.

This is potentially a big project, but it can be broken down into small, easy-to-complete pieces. If you have any interest in these issues, please contact one of the Task Force co-chairs, Lois Mermelstein or Juliet Moringiello.

**Updates from the International Trade Subcommittee**

*Co-Chairs John Gregory and Hal Burman*

The International Trade Subcommittee considered a number of international initiatives on which its input can be useful if given soon. These included two products of UNCITRAL:

1. The Electronic Communications Convention of 2005, which may go before the Senate for consent to ratification shortly. At the WWM, the subcommittee reviewed a draft submission of the treaty to the Senate. The submission is being redrafted based on the breakout meeting discussions, which were followed up by conference call on January 31. A further call will be held in mid-February among those who have expressed an interest.

2. The current work on electronic transferable records (ETR) continues. A draft model law has just been circulated (January 31) for expert input before being revised for discussion at the next meeting of the Working Group in May. The meeting considered the policy dynamics of the ETR work. The subcommittee will be looking for short-term input on the draft model law, which will probably be done by a series of conference calls.

The subcommittee also noted the work of the UN Committee on Trade Facilitation (CEFACT) in its work on interoperability guidelines for 'single window' operations (to consolidate customs clearances and facilitate cross-border transportation and import-export trade) and on authentication. The meeting took a strong view that any such guidelines should be technology neutral, to avoid restricting innovation in the future. Opportunities to comment on the current drafts on both projects will be offered via the subcommittee's listserv and webpage in the near future. The single window project may also be the topic of discussion at the Spring meeting in DC, where similar concurrent efforts in various regional bodies around the world raise the potential for action to occur, which is both an opportunity and risk for North American interests.

Members of the subcommittee may get involved by responding to appeals for help to the list, or pre-emptively by contacting either co-chair, Hal Burman or John Gregory, whose contact information is found on the [subcommittee webpage](http://apps.americanbar.org/buslaw/committees/CL320000publnewsletter/201302/).
**Project on Criminalization of Intellectual Property**

*Cathy Gellis*

The Committee used a well-attended breakout session at our Winter Working Meeting to kick off a new project focusing on the increasing criminalization of intellectual property disputes, headed up by Sausalito-based Cathy Gellis. The group will focus first on two projects. Cathy will assess planning a panel presentation for the ABA annual meeting in San Francisco in August. Jamie Clark will spearhead development of a primer for business lawyers to identify, prepare for, and respond to government actions taken against clients' technology use and development. Please let Jamie know if you are interested in helping out with this project. Contact Cathy if you have any project ideas or would like to participate in the group.

**Update from the Cybersecurity Subcommittee**

*Co-Chairs Roland Trope and Tom Smedinghoff*

Stephen Humes, a partner at Holland & Knight and a member of the ABA Section of Environment, Energy & Resources, and Roland Trope (contributing by phone) presented a CLE session on *Legal Duties Arising from Cyber Attacks on the Grid*. Their presentation included discussion of the issues and challenges that would be presented by a forthcoming Executive Order on Cybersecurity. A copy of a deliberative draft of the Executive Order, together with the CLE PowerPoint slides and essay, are on the subcommittee's website.

During the WWM breakout sessions, the Cybersecurity Subcommittee decided, as a new project, to respond to the forthcoming Executive Order on Cybersecurity and the two information sharing notices it contemplates the Department of Homeland Security (DHS) will send to enterprises. One notice will inform an enterprise that intelligence reports show that it is among the targets of a cyber attack aimed at the U.S. homeland. (We refer to it as an "Imminent Target Notice.") The other notice will inform owners and operators of certain critical infrastructure enterprises that if a cyber attack damages their company, the result could be "catastrophic regional or national effects on public health or safety or economic security or national security." (We refer to it as a "Catastrophic Target Notice.")

The new project is premised on the view that a company that receives either an Imminent Target or Catastrophic Target Notice (or both) will be confronted with a host of significant legal issues that it will need to address and will probably want to prepare in advance to address. Some of the issues will be raised by other provisions in the EO, some by existing regulations (such as the SEC Staff Guidance on Cybersecurity disclosures), and others may involve enhanced precautions and contractual provisions that such notices might trigger. The project will seek to respond to such issues by preparing a guide for legal counsel to recipients of the DHS notices.

The near-term plan is to develop a detailed outline for the Guide by the end of March 2013,

in order to have a working session on the Guide at the ABA Business Section's Spring Meeting in Washington, DC April 4 - 6, 2013. The meeting will have a telephone link so that persons who cannot attend the Spring Meeting, but wish to participate in the working session, can do so remotely. If you were not at the breakout planning session for this project, but are interested in working on it, please send your name and contact information to Roland Trope.

**Update from the Digital Media Subcommittee**

*Co-Chairs Jon Garon and Susan Stephan*

The Digital Media Subcommittee met in Los Angeles and welcomed a number of first-time attendees to the working session. Although the subcommittee will not hold a meeting at the Spring Business Law Meeting, there was a good deal of discussion regarding potential upcoming projects. For each of the projects listed below, the subcommittee is seeking lead authors and webinar speakers. If you are interested, please contact Jon Garon or Susan Stephan.

1. Monitoring the Changes to Publishing. 2012 may one day be viewed as the year the book went digital and publishing was reinvented. A convergence of challenges to publishing Fair Use and First Sale doctrines, industry consolidation, antitrust consent decrees, massive
ebook adoption, and changing expectations by publishers of the rights they acquire has made this a time of dramatic change for publishing.

2. Licensing Digital Content for Mobile. The subcommittee discussed the content/technology divide and the need to clarify the rights and obligations to content rights holders of the impediments to effective content licensing.

3. Updating Principles for End User License Agreements. The subcommittee discussed the ongoing changes to regulations such as COPPA and public frustration regarding end user license agreements (EULAs). While there was recognition that no ABA section or committee may publish a statement on acceptable business practices, there was consensus that providing a set of principles regarding the development of EULAs would benefit both business and consumers.

Update from the Mobile Commerce Subcommittee
Co-Chairs Richard Balough and Theodore Claypoole

The mCommerce Subcommittee hosted a panel discussion at the WWM on the Bring Your Own Device (BYOD) Movement and the business lawyer's role in protecting her clients who implement a personal device regime into the enterprise. The subcommittee is developing a white paper to assist business lawyers in identifying risks and issues as they help their clients with BYOD policy implementations. Development of the white paper will be separated into discrete parts so that individuals can contribute to specific areas of the document. The subcommittee will post the working draft for collaboration on Box. Anyone interesting in working on the BYOD guidelines should contact one of the co-chairs, Ted Claypoole or Richard Balough, for access to the mCommerce folder on Box.

Update from the Electronic Financial Services Subcommittee
Co-Chairs Edward Morse and Stephen Middlebrook

The Electronic Financial Services Subcommittee is exploring several possible projects. One involves EMV technology (a global standard for credit and debit payment cards based on chip card technology. As targeted dates by the card brands for processing EMV transactions (April 2013) and retail accommodation and use (2015) are fast approaching, the transition between traditional magnetic stripe systems and EMV (sometimes called, albeit inaccurately, "chip and pin") will present the need for new equipment and new knowledge for retailers and their lawyers about the risk of operating in this environment. The subcommittee discussed the possibility of developing a white paper, brochure, or other appropriate guidance so that retailers and their lawyers can understand the rules associated with EMV, the locus of the risk of fraud in this environment associated with various authentication methods for card ownerships, and the continuing role of PCI DSS (Payment Card Industry Data Security Standard) for protecting card information in the processing chain.

Another topic of interest is "Payment Cards at the Border." The Financial Crimes Enforcement Network (FINCEN) has proposed rules that require travelers to declare the value of prepaid cards, along with cash and other financial instruments they may be carrying when they leave or enter the United States. The group discussed the technical and legal issues presented by these requirements, including privacy and due process concerns, definitional ambiguity, and other legal objections and/or obstacles to implementing such a rule. We decided to continue this discussion at the Spring meeting in Washington, DC, and to invite appropriate guests from the card industry and/or government to explore further this issue. For a recent article and links to the proposed rules, see a recent article in Payments Journal. Those interested in working on either of issues should contact Ed Morse or Steve Middlebrook.

Internet Governance Task Force Update
Chair David Satola

Readers will recall that the our last update dealt with our recommendation, under ABA blanket authority, to the US Government to ensure protections of basic human rights online as part of the treaty-making process at WCIT-12 in Dubai. WCIT-12 has come and gone, but the debate over human rights and the Internet is far from over. The result of the international treaty-drafting conference resulting in new "International Telecommunication Regulations" (ITR) was ambiguous and inconclusive. After first claiming that Internet Governance issues would not be
included in the new ITRs, the International Telecommunications Union (ITU), the UN body running WCIT-12, allowed an 11th-hour submission of a Russian-sponsored "non-binding" resolution, innocuously entitled "To Foster an Enabling Environment for the Greater Growth of the Internet", to be appended to the new treaty. Some 52 countries, including the US, voted against or abstained from voting on the treaty (89 voted in favor). The resolution suggests a departure from the "multi-stakeholder" approach that currently defines Internet Governance and, in the eyes of many portends, instead, an inter-governmental (i.e. state-centric) approach to regulating the Internet and the suppression of privacy and free-speech rights on the Internet. Whereas previous ITRs enjoyed the support of nearly every country, we now have the curious situation of the existence of a "treaty" without the participation of countries which most of the world's major Internet suppliers and operators call home. It is likely that these ITRs will continue - possibly in a manner similar to the ongoing WTO trade talks - to be negotiated over the coming years.

**Consumer Protection Subcommittee Update**

*Co-Chairs John Rothchild and James Nehf*

The Consumer Protection Subcommittee met to continue work on its project to update the Safeshopping.org website. We reviewed a draft revision of one section, agreed on a revised organization of the topics to be covered, added a few topics, settled on a format for each section, and divided the next stage of work among subcommittee members. John Rothchild also made a presentation on the Federal Trade Commission's effort to update its Dot Com Disclosures guidance for the first time since its issuance in 2000. The revised guidance, which will address disclosures in social media and on mobile devices, is expected to be released very shortly (though its release date has already been delayed once). The subcommittee will review the guidance when it is available and assess whether it may serve as the basis for a future project.

**Cyber News You Can Use**

**Brazil's New Law on Electronic Crimes**

*Renato Opice Blum, Attorney, Economist, and President of the IT Advisory Board of Fecomercio*

After 15 years of discussion, Brazil's government has enacted a long-awaited law, 12.737/2012, that defines computer-related crimes and covers important issues such as electronic device invasion, unauthorized remote access, and interruption of web services. The law limits the definition of invasion to cases in which an "infringement of security mechanisms" occurs, excluding computer devices without protection mechanisms.

However, the law's language raises some ambiguities. The expressions "security mechanism" and "computer device" (only hardware, what about software?) are not defined. Furthermore, because "invasion" suggests "entering forcefully," cases of inappropriate acquisition of data through social engineering techniques and other means (e.g., disclosure of password by the owner to third parties) theoretically would not be included in the newly born classification. Such actions would not constitute violation, but merely unauthorized access. Additionally, it is possible to foresee a broad debate about who would be the "owner of the dispositive" invaded - expression used to designate the victim. The legal text seems to refer only to the owner, not clarifying if an eventual possessor or user could also be protected. As well, penalization of the disclosure of industrial secrets obtained by invasion appears duplicative because such improper disclosure is already considered a crime under the Protection of Industrial Property Law (Law 9.279/96).

The sentences imposed appear to be quite soft, allowing the enforcement of the conditions of Special Courts' proceedings. This is noteworthy because the international trend is precisely the opposite. For example, it recently became news that California sentenced a hacker to 10 years of prison for stealing pictures from celebrities through the web - in addition to restitution of $76,000. This aspect of the law, which was created after many years of debate, is puzzling because in the majority of computer crimes the material loss is just a small part of the problem: the damage occurs within the intimate sphere of private lives or concerns sensitive business information, making the lost data invaluable to the victim.
Recent Developments in Cybersecurity
Cybersecurity Subcommittee Co-Chairs Roland Trope and Tom Smedinghoff

There are two developments related to cybersecurity contained in the 545-page National Defense Authorization Act 2013 ("NDAA 2013" or the "Act"):

(a) Penetration Reporting Becomes Mandatory. On January 2, 2013, President Obama signed into law the NDAA 2013. Section 936 of the Act imposes a new cybersecurity requirement on "cleared defense contractors" - those defined in the Act as "a private entity granted clearance by the Department of Defense to access, receive or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense." (§ 941(e)(1)) The Act requires such defense contractors (and presumably "cleared" subcontractors at every tier) to submit to the DoD "rapid reports" of "successful penetrations" of network or information systems that the DoD will identify or designate at such contractors. Each "penetration" report must contain (a) a description of the technique or method used in the penetration, and (b) a sample of the malicious software, if discovered and isolated by the contractor. (§ 941(d)) In addition, such contractors must grant DoD personnel post-attack access to equipment or information of the contractor "necessary to conduct a forensic analysis to determine whether information created by or for" the DoD in connection with any DoD program "was successfully exfiltrated from a network or information system of the contractor, and if so, what information was exfiltrated." Although the Act does not mention it, if a "cleared defense contractor" happens also to be publicly owned it would also need to consider what, if any, disclosure it would need to make in compliance with the SEC Staff Guidance on cybersecurity (issued in October 2011).

It should also be noted that last year's NDAA set a deadline of October 2012 for issuance of a cybersecurity-related set of regulations, namely those for the detection and avoidance of counterfeit electronic parts in equipment delivered to the DoD. The deadline passed without issuance of the regulations, but it is reasonable to expect that such regulations will appear in the Federal Register within the next few months. The regulations will require defense contractors to create extensive compliance programs that will probably cause significant cost increases, not only to create, implement, and audit the compliance programs, but to cover the costs that will be incurred as "suspected parts" are identified and removed from the supply-chain and contractors limit their purchases to comply with DoD requirements to procure only from "trusted suppliers." The regulations, which will probably focus also on firmware updates from offshore, are part of a larger Congressional concern to safeguard the supply-chain for equipment designed, developed and manufactured for the U.S. Government.

(b) DoD to Develop Contract Clauses for Obtaining Higher Quality Software. The NDAA 2013, Section 925(e), requires the DoD to study potential mechanisms to obtain "higher quality and secure development of computer software" for the Department. The mechanisms may include "(A) Liability for defects or vulnerabilities in software code," and "(B) So-called 'clawback' provisions on earned fees" that would enable the DoD to "recoup funds for security vulnerabilities discovered after the software is delivered." If such study results in the crafting of software acquisition contract clauses along those lines, it would constitute a significant departure from the software industry's long-standing business model which typically treats the vendors as not liable for such security shortcomings.

Presentations and Publications of Interest

Governments Control the Internet

John Gregory, co-chair of the CLC International Trade Subcommittee, recently published in Slaw, Canada's online legal magazine, a note on how governments control the Internet, especially on opportunities for censorship. You can read it here.

Cyberlaw Gigs
This new section of the Cyberspace Law Committee Newsletter will include job postings for or by committee members. Please send all postings to Communications Co-Directors Cheryl Balough and Lois Mermelstein by the 20th of one month for posting in the following month's newsletter.

Your Articles Are Welcome

We are always looking for fresh and relevant content for the CLCC newsletter. Have you written or presented on something your fellow committee members would be interested in? Let them know! Email your contribution to committee Communications Co-Directors Cheryl Balough and Lois Mermelstein.

back to top