Cyberspace Law Committee

Message from the Chair

Committee on the Law of Commerce in Cyberspace - What's in a name?

Some of you know that the full, original name of this committee is the Committee on the Law of Commerce in Cyberspace. I recently pondered the strange acronym in the committee's mailing list - the CLCC-MEMS list - and wondered why we needed the extra C. One of my esteemed predecessor chairs explained: some years ago this committee was incubated by the UCC committee. The CLCC founding fathers and mothers were interested in the ways that commercial transactions would be analyzed as businesses began to form contracts and conduct transactions online.

These days, we are still interested in how the online context informs the analysis of business transactions and contract formation. Our explorations have expanded beyond the UCC, but the focus is still largely commerce. How should businesses secure new domain names and manage conflicts with trademarks and domains? How can they effectively and safely protect and expand business globally through social media? Where are the next major threats to businesses' digital security? Where are the significant legal risks and pitfalls in shifting business assets and processes to the cloud? These are just some of the commercial issues we are exploring as our members consider how businesses can most effectively navigate the increasingly complex global digital world.

Stay tuned for more news from the committee on plans for our upcoming 2012 Institute on the Law of Cyberspace and Winter Working Meeting, January 20-21 in San Francisco. We will have programming on a great variety of cyberlaw issues and lots of opportunities for committee members, old friends from the CLCC days and newbies alike, to join roundtable discussions and planning sessions on new committee book and article projects, CLE programming, and other cyberlaw content. Social events and additional plans will be announced soon.

Jonathan T. Rubens
Chair, Cyberspace Law Committee, Business Law Section
Jonathan.Rubens@leclairryan.com
Discounted airfares are available from ABA Orbitz for Business. To book online, follow these steps:

2. Click under the Orbitz for Business logo at the top of the page,
3. Click on the appropriate link in the Travel Paid by Self box.

For assistance with online or offline reservations, call toll free 1-877-222-4185.

**NOTE:** Please make travel arrangements for an arrival on **Thursday, January 19**. The meeting will officially begin first thing on **Friday** morning.

*We hope to see you in San Francisco!*

### Other Programs of Interest

**November 1:** Using Social Media in Discovery: Avoiding Ethical Landmines. For more information and to register, click [here](#).

**November 2:** Green IP: An Overview of Opportunities and Risks. For more information and to register, click [here](#).

**November 16:** John Gregory, co-chair of the International Trade Subcommittee, is giving a one-hour teleconference tutorial on electronic transferable records for the Information Technology Lawyers of Canada ([IT.Can](https://www.itcan.org)).

**November 16:** The Bully at School Goes High Tech: Protecting Students in the Internet Age. For more information and to register, click [here](#).

**November 17:** The America Invents Act: Key Facts You Need To Know Now About Provisions that Are Already Law. Sponsored by the ABA Section of Intellectual Property Law. Registration details are available [here](#).

**November 29:** New Restrictions on U.S. Internet Sales: Data Passes, Negative Options, Automatic Renewals and Recurring Charges. For more information and to register, click [here](#).

**March 1-2, 2012:** 2-Day Symposium on Law & Informatics, hosted by Northern Kentucky Law Review and Salmon P. Chase College of Law, Highland Heights, KY. March 1: day-long CLE program regarding practical solutions to current problems facing attorneys and clients. March 2: Law Review Symposium, an opportunity for academics, practitioners, consultants, and students to exchange ideas and explore emerging issues in informatics law, disruptive innovation, and the increasingly interconnected information environment. Committee member Jon Garon is the Symposium Faculty Sponsor; other committee members are among those presenting. For more details, visit the [symposium website](#).

### Cyber News You Can Use

**Who Is Applying for New gTLDs?**

*Erik Pelton, Chair of Marketing & Advertising Subcommittee*

A broad variety of entities are applying to create new generic Top-Level Domains (gTLDs). Several websites provide lists of the applicants:

- [http://registries.tel/](http://registries.tel/)
- [http://www.newdomains.org](http://www.newdomains.org)
- [http://valideus.com/resources/gtlds-list/](http://valideus.com/resources/gtlds-list/)
Do Not Track Regulation and Behavioral Advertising
John Rothchild and James Nehf, Co-Chairs of Consumer Protection Subcommittee

In December 2010, a Federal Trade Commission staff report proposed a “do not track” mechanism for consumers, enabling them to prevent the collection of information about their online activities. This information is used to support online behavioral advertising—that is, advertising tailored to a particular individual based on what the consumer thinks she knows about her interests and preferences. Much controversy has resulted. FTC Commissioner Thomas Rosch reviewed many of the issues in a speech at a Chicago gathering of antitrust lawyers on October 14, 2011. Rosch expressed skepticism about the self-regulatory approaches to do-not-track that various players in the online advertising industry have rolled out, finding them inadequate in several respects. He examined the mechanisms in three web browsers (Firefox, Chrome, and Internet Explorer) and one devised by an industry group called the Digital Advertising Alliance. Rosch also reviewed proposed legislation to mandate do-not-track that is currently pending in Congress. The speech is here.

Privacy Policies for Mobile Apps
Ted Claypoole and Richard Balough, Co-Chairs of mCommerce Subcommittee

The Mobile Marketing Association has issued a proposed model Mobile Application Privacy Policy Framework for mobile applications developers. The framework is intended to give mobile applications developers clear language for disclosing to users what data is collected and used by mobile applications. The framework proposes language that answers the following questions:

- Do third parties see and/or have access to information obtained by the application?
- Does the application collect precise real time location information for the device?
- What is the data retention policy for the information?
- What information is collected about children?
- What level of security is provided for the data collected?
- What are the opt-out options?

The association is taking public comments on the policy until November 18, 2011, after which time it will issue a final model policy. The framework is available here.

The Mobile Marketing Association is a trade association for mobile marketing and associated technologies.

Cautionary Marketing Tales
Erik Pelton, Chair of Marketing & Advertising Subcommittee

In our digital social-media age, brands can rise and grow rapidly but they can fail even faster. Last month, the hugely popular and successful DVD and online video service Netflix announced a new brand name - Qwikster - for its DVD service. The move was curious and questioned by many. Until this year, the Netflix brand was charming and could do no wrong. This bungle is sure to have scuffed the brand’s image. Netflix has since realized the error of its ways and recently announced that Qwikster is no longer. Perhaps the Qwikster brand name will still be used by Netflix in some manner, but at least as a separate service that would require separate accounts and logins for users, Qwikster is gone. Has Netflix righted the ship soon enough to avoid real damage? Only time will tell.

Recent times have seen a rash of brand mismanagement. Twitter is entangled in several disputes due to its delay in protecting all its trademarks after it launched a few years ago. Google, one of the most valuable companies in the world, has failed to protect all of its brand names and logo. The University of Colorado recently spent more than $700,000 on a minor logo change. The good news is that our clients can learn from the mistakes of others and avoid making the same blunders.
Potential of Cyber Attack on U.S. Electric Grid
Roland Trope and Tom Smedinghoff, Co-Chairs of Cybersecurity Subcommittee

On October 12, 2011, the Financial Times carried a story on the threat of cyber attack to the U.S. electrical power grid. The graphic in the story describes a form of attack that would resemble in several features the Stuxnet attack on the Iranian uranium enrichment facilities at Natanz where the targets were the spinning centrifuges - and in the FT's story the target would be the electrical power plant's spinning turbines.

Check Out MIRLN for More Information

Vince Polley continues to publish MIRLN (Miscellaneous IT-Related Legal News) every three weeks. Subscriptions are free. It's also online at http://www.knowconnect.com/mirl and at the bottom of eBLT (under the heading "OTHER NEWSLETTERS BY SECTION MEMBERS"). Take advantage of this wonderful resource.

Updated Reg E Booklet
Hank Judy and Sarah Jane Hughes

On October 24, the Office of the Comptroller of the Currency (OCC) updated its Electronic Funds Transfer-Regulation E booklet, which is part of the OCC Comptroller's Manual. It contains a concise description of the new regulations on gift cards promulgated under the authority of the CARD Act of 2009. See pages 15-17 of the booklet.

CLC Projects

International Rules for Electronic Transferable Records?
Hal Burman and John Gregory, Co-Chairs of International Trade Subcommittee

The E-Commerce Working Group of the UN Commission on International Trade Law recently met in Vienna to discuss the possibility of an international legal regime for electronic transferable records. The Working Group had before it a useful Working Paper (WP.115) on the issues. Some thought the agenda was to create an international version of section 16 of the UETA on that topic. To resolve the issues of uniqueness, transfer, authentication and enforcement, the Working Group also considered the creation of one or more international registries. Whether the same legal regime would work for documents of title (bills of lading etc) and for financial documents (chattel paper) was the subject of some debate. Also much debated was whether there was any real commercial demand for such legal rules; a number of countries (though not the US) said no. The Working Group may meet again in February 2012 if the appropriate supporting documents can be prepared in time for translation and circulation before then.

The UN Working Group also briefly discussed a proposal from a technical working group of the United Nations Center for Trade Facilitation (CEFACT) on 'digital evidence certificates.' The Working Group asked to have a chance to analyze the document formally, as it appeared to have a number of defects in its statement of legal impact of the proposed technology. See here for John Gregory's discussion of the high-level issues in this matter, as well as some of the specific flaws in the CEFACT document.

Draft Report on Legal Framework for Online Identity Management
Roland Trope and Tom Smedinghoff, Co-Chairs

Tom Smedinghoff completed and is circulating for comment an 85-page draft report of the Identity Management Legal Task Force: Building the Legal Framework for Online Identity Management. Tom welcomes readers and comments on the draft; if you are interested, please contact Tom.
SEC Guidance Issued on Disclosure
Roland Trope and Tom Smedinghoff, Co-Chairs of Cybersecurity Subcommittee

In May 2011, five Senators asked the SEC to issue guidance and require disclosure of cyber attacks that cause loss of a company's intellectual property. In response, the SEC Division of Corporate Governance issued on October 17, 2011, CF Disclosure Guidance: Topic No. 2 - Cybersecurity. The Guidance is not a rule, regulation, or statement of the SEC, but it does express the views of the Division, which is responsible for interpreting existing rules and proposing new rules. The Guidance is intended to assist registrants in assessing what, if any, disclosures should be provided regarding cybersecurity matters.

The Division notes that "no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," but "a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents." Moreover, material information concerning such risks and incidents "is required to be disclosed when necessary in order to make other required disclosures ... not misleading."

As such, the Guidance is a significant interpretive release by the Division, and it would not be prudent for companies to ignore it or treat it as not applicable to them because they have not, to their knowledge, experienced a cyber attack. As an official at McAfee recently observed, there are only two kinds of companies - those that know that they have been compromised by cyberattacks and those that don't.

One of the most significant features of the Division's Guidance is that unlike other government initiatives that have tried with little success to legislate cybersecurity measures or standards, the Guidance requires public companies to disclose the extent to which such companies have demonstrable deficiencies in cybersecurity. For the investing public, such information is clearly material. However, the Guidance appears to have allowed its efforts at prompting such disclosures to overstep the measure, because some of the disclosures it advises companies to make would undermine a company's cybersecurity by providing precisely the sensitive cyber defense information that an adversary seeks in order to plan and execute a cyberattack on the enterprise. For example, the Guidance recommends that, depending on the registrant's particular facts and circumstances (and to the extent material), appropriate disclosures may include:

- Risks related to cyber incidents that may remain undetected for an extended period. (Surely a company should be loath to disclose such information because an adversary would take advantage of it.)
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences. (Here the need to report such incidents is compelling, but the Guidance should make clear that registrants may comply with such guidance without disclosing details of what vulnerability the attack exploited.)

Overall, the Division's Guidance would appear likely to have a greater influence on companies and their investment in cybersecurity than any of the stovepipe regulations that have preceded it.

Most importantly, the Guidance reflects the emerging trend of a convergence between legal issues of cybersecurity and legal issues concerning securities and the investing public. Clients and counsel will need to adjust to this convergence in order to fulfill obligations set forth in the Division's Guidance.
explosion of content, brands, and intellectual property, yet businesses often fail to properly use and/or protect all of their trademarks and copyrights. Some simple steps can enhance both the legal protection and practical value of this intellectual property: use proper copyright and trademark notices, use trademarks in a manner that sets them apart from other text, register core intellectual property assets, and set up free Google Alerts to monitor for misuse by others.

Cyberspace Impact of Municipal Bankruptcy

Longtime committee contributor and leader Professor Juliet Moringiello has been busy providing media commentary on Harrisburg, Pennsylvania's bankruptcy filing. She also testified before the Pennsylvania legislature on October 20 about using Chapter 9 bankruptcy to resolve municipal financial distress. It is remarkable that a city of this size and import (a state capital, no less) has filed for bankruptcy protection (Orange County, CA redux?) but one wonders about the cyberspace impacts - does anyone, a judge or a trustee perhaps, take over the city's web sites and online communications systems? The answer is "no": a city remains in complete control of its property in bankruptcy - because of Tenth Amendment concerns, no trustee is appointed in a Chapter 9 bankruptcy and the judge's power over a city is limited.

Ethical Issues for Lawyers Using Social Media

Sarah Jane Hughes, committee publications director, and Roland Trope, co-chair of the Cybersecurity Subcommittee, are about to publish a long article in William Mitchell Law Review on lawyers' professional responsibility and social media, principally using cloud computing. The article covers the New York Rules of Professional Conduct, the model rules, the ABA Ethics 20/20 proposal, and NIST's 2011 guidance. The article is entitled Red Skies in the Morning: Ethical Considerations at the Dawn of Cloud Computing. Sarah Jane and Roland thank Chris Kunz for suggesting their names to the editors.

International Legal Frameworks for Cybersecurity

Hank Judy, co-chair of the Internet Governance Task Force, gave a lecture on October 17, 2011, to the Cybersecurity Graduate Program at the University of Maryland Baltimore Campus on the subject of International Cybersecurity Legal Frameworks and Internet Governance. He reports that the work of the Computer Law Committee was liberally mentioned, and he thanks Roland Trope for generously sharing slides on a related subject.

Disruptive Innovation

Jon Garon, co-chair of the Digital Media Subcommittee, recently presented Mortgaging the Meme: Lessons for Financing Disruptive Innovation, which is available for free download. The presentation was previewed at the University of Dayton Law School on Sept. 21, 2011 and presented at the International Business Law Conference in London, Sept. 24, 2011.

What is disruptive innovation, you ask? Disruptive innovation can be described as the introduction of a new conceptual idea or meme into an existing system that causes the system to be fundamentally altered. Assembly lines, air conditioning, digital film, and personal computers represent such innovations, all of which led to fundamental paradigm shifts. The convergence of globalization, a networked economy, and digital technologies have made disruptive innovation a threat in almost every industry. Changes to publishing, music, and television distribution - along with the rise of social media - highlight this transformation, but they are not alone; manufacturing, retail, payment systems, transportation and other industries are

Disruptive innovation, however, follows predictable patterns. Investors can
You are receiving this Committee Newsletter because you are a member of the ABA Business Law Section Cyberspace Law Committee. To opt-out of this publication, please visit the ABA Subscription Portal.

You can access the Cyberspace Law Committee website here.

Your e-mail address will only be used within the ABA and its entities. We do not sell or rent e-mail addresses to anyone outside the ABA.

Update your profile | Unsubscribe | Privacy Policy

American Bar Association: 321 N Clark | Chicago, IL 60654 | 800-285-2221

Business Law Section: 312-988-5588 | Section Staff | businesslaw@americanbar.org | www.abusinesslaw.org

Copyright © 2011

anticipate these shifts if their financial transactions are properly structured and effectively documented. The model requires a holistic intellectual property approach which looks beyond just patents. It must explicitly incorporate the underlying meme, and it must account for the inflection points in the transformation pattern. Utilizing this model, inventors, private equity investment structures and established firms can maximize value and promote innovation. This article provides an overview of disruptive innovation from examples of the past decade, identifies the underlying patterns of change common to disruptive innovation, and highlights strategies to mitigate disruption for existing industries, while addressing the intellectual property securitization aspects to structure effective deals for both the investors and innovators.

New Updates to Canadian Privacy Act

Committee member Lisa Lifshitz recently co-authored an article discussing the Canadian government's proposed updates to PIPEDA, the Canadian federal private sector privacy act. Now pending in Canada's Parliament, the bill redefines "personal information" to remove the provision that business contact information is not personal information. It clarifies the meaning of the "valid consent" required to collect, use, or disclose personal information. The bill allows exceptions for the use of personal information in a business transaction and in conjunction with an employment relationship. The bill also introduces a mandatory breach notification procedure. You can access the full article.

Cybersecurity Risks to Electric Utilities

Roland Trope, co-chair of the Cybersecurity Subcommittee, gave a one-hour presentation at the Edison Electrical Institute (EEI) Fall 2011 Legal Conference in San Francisco on October 17, 2011. EEI members are the major electrical and nuclear power utility companies, and participants in the conference were the general counsel of these enterprises. The topic was A Porous Enterprise: Cyber Security Risks to Electrical Utilities from Web 2.0 and Cloud Computing. Because the SEC's Guidance came out that afternoon, Roland also presented a brief look at the significance and challenges of the Guidance for conference participants.

Your Name Here

Want to be in this newsletter? Have you written or presented on something your fellow committee members would be interested in? Let us (and them) know! Email your contribution to committee Communications Directors, Cheryl Balough (cbalough@balough.com) and Lois Mermelstein (lois@loismermelstein.com).