Message from the Chair

Here in California it feels like the continued skirmishes in the War between The North and The South (Silicon Valley vs. Hollywood) as the blogs buzz over the threat of new Internet legislation. First the Senate weighed in, at the Southerners' behest with the Protect IP Act ("Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011"), and then came the House's tougher effort, SOPA (the "Stop Online Piracy Act"), supplying more extensive civil procedural tools and causes of action to combat Internet piracy and intellectual property theft. Northern detractors critique both bills as further overreaching by Big Content to the detriment of an economically robust Internet and individual freedoms. This week we were reminded that these battles have national and international implications, as famed consultancy Booz released a report confirming the widely-held Silicon Valley view that SOPA would be a death-knell for tech innovation. The report's conclusion: a "large majority of the angel investors and venture capitalists who took part in a Booz & Company study say they will not put their money in digital content intermediaries (DCIs) if governments pass tough new rules allowing websites to be sued or fined for pirated digital content posted by users." You can read Booz's press release [here](#). We'll be watching the battles closely, through the end of the year and on into 2012.

Come to the Committee's Winter Working Meeting and Institute on the Law of Cyberspace, January 20-21 in San Francisco, for a recap of these battles and some theorizing and prognostication over what we'll see next. And lots of discussion on many other cyberspace topics to boot (see more info below). There's still time to plan your trip to SF, and keep your eyes open for more news about special plans and speakers for the meeting. Meanwhile, happy holidays.

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

Upcoming Programs, Events and Projects

Cyberspace Law Institute and Winter Working Meeting Update

We're very pleased to let you know about some of the exciting programming to be offered at the Committee's 2012 Institute on the Law of Cyberspace and Winter Working Meeting, **January 20-21, 2012**, at the Hotel Kabuki, San Francisco. We will offer 4+ hours of CLE programming on a diverse set of cyberspace topics, including:

- What happens to your social media accounts, email passwords, and digital authentication devices when you die?  
- Updates on the coming new generic top level domains, including advice you can give your clients  
- Mobile applications and geolocation: To what extent do the First and Fourth Amendments protect US Citizens from certain government tracking?

The meeting will also feature a block of hosted roundtable discussions on current/cutting-edge cyberspace topics. We're sure to be addressing some of the important current issues in the area, such as:
Cybercrime, including recent SEC guidance on data outsourcing
- DMCA case review, including specific discussion on safe harbor elements.

Registration for the meeting is open! Sign up now. Deadline for registration is January 6.

Hotel Kabuki is also currently accepting reservations at a room rate of $139.00 + tax (until January 5, 2012). To book accommodations, please call the hotel directly at 415.922.3200 or 800.553.4567 and refer to the "ABA Cyberspace Law Institute" or go online to the hotel website. Discounted airfares are available from ABA Orbitz for Business. Plan to arrive on Thursday, January 19, because the meeting begins first thing Friday morning.

Kristine Dorrain
Programming Director
kdorrain@adrforum.com

Other Programs of Interest

December 13, 2011 - eDiscovery without Borders

The ABA Section of Science and Technology Law is presenting a brown bag program in Washington, DC at the American Association for the Advancement of Sciences. A distinguished panel, including the Cyberspace Law Committee's Stephen Mason, will answer questions like: Does the physical location of the information dictate the laws and regulations governing access to the data, or does the location of the portal for the cloud services determine what is permitted? For more information, click here.

January 25, 2012 - Webinar: Non-traditional Trademark Protection in the U.S.

What do blue football fields (Boise State University), brown delivery trucks (UPS), marching ducks (Peabody Hotels), outdoor lighting displays (Holiday Inn), and a Statue of Liberty costume (Liberty Tax Service) all have in common? They are all non-traditional trademarks registered with the U.S. Patent and Trademark Office. So too are a variety of sounds, colors, and even scents. Registration of non-trademarks in the U.S. has increased significantly in recent years. This webinar, presented by the Association of Intellectual Property Firms (AIPF), will explore the history of non-traditional trademark registration, along with the legal and practical issues involved. We will also survey the spectrum of non-traditional trademarks that are protectable and review special considerations for the application process involving non-traditional trademarks. More information is available here. You can also contact Erik M. Pelton at erik@erikpelton.com for more information.

March 1-2, 2012 - Law and Informatics

This two-day Symposium on Law & Informatics is hosted by the Northern Kentucky Law Review and Salmon P. Chase College of Law, Highland Heights, Kentucky. 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

Supreme Court Considers Geolocational Privacy
Ted Claypoole and Richard Balough, Co-Chairs of mCommerce Subcommittee
The extent to which the U.S. Constitution gives individuals any geolocational privacy was argued in early November before the U.S. Supreme Court. The case, United States v. Jones, involves whether the government is required to obtain warrant to track an individual 24 hours a day for 28 days using a GPS tracking device that sent out a signal every 10 seconds. The device was placed on the individual's car without a warrant. The appellate court threw out a conviction finding that the use of the GPS tracking device for such a length of time required a warrant. During the oral argument, Justice Breyer told the government, "If you win this case, then there is nothing to prevent the police or government from monitoring 24 hours a day the public movement of every citizen of the United States. And-and the difference between the monitoring and what happened in the past is memories are fallible, computers aren't. . . So if you win, you suddenly produce what sounds like 1984." Justice Alito speculated that if "we look forward 10 years, and maybe 10 years from now 90 percent of the population will be using social networking sites and they will have on average 500 friends and they will have allowed their friends to monitor their location 24 hours a day, 365 days a year, through the use of their cell phones. Then-what would the expectation of privacy be then?" A copy of the transcript is available here. Geolocational privacy as it relates to mobile devices and mCommerce is one of the areas that the mCommerce subcommittee will discuss at the Winter Working Meeting in January and will follow during 2012.

Facial Recognition Technology Moves from Sci-Fi Thrillers to Your Local Watering Hole
Ted Claypoole and Richard Balough, Co-Chairs of mCommerce Subcommittee

The New York Times recently ran an article discussing the realities of facial recognition technology and social media, including an interesting discussion of privacy and other legal concerns.

Are Medical Devices Susceptible to Hacking?

In late October, The Register ran another story about a real-life sci-fi thriller: "Insulin Pump Hack Delivers Fatal Dosage Over the Air". It recounts the success of a researcher, who last year showed how to take control of two widely used models of ATMs, in taking over insulin pumps that allow patients and doctors to adjust the pumps' functions.

Net Neutrality
John Rothchild, Co-Chair of Consumer Protection Subcommittee

Mid-November contained a good week for net neutrality. On November 10, Republicans in the Senate lost a 52-46 vote on a resolution that would have repealed the FCC's net neutrality rules under a little-known procedure established by the Congressional Review Act of 1996. The rules, which were promulgated in December 2010, are set to go into effect on November 20. Get more details here. Meanwhile in the European Union, on November 17 the European Parliament passed a resolution favoring net neutrality, asking the European Commission to "ensure that internet service providers do not block, discriminate against, impair or degrade the ability of any person to use a service to access, use, send, post, receive or offer any content, application or service of their choice, irrespective of source or target." Read more here.

Update on Cloud Computing Security
Roland Trope and Tom Smedinghoff, Co-Chairs of Cybersecurity Subcommittee

On October 17, 2011, the GAO issued its decision in Matter of Technosource Information Systems, LLC; TrueTandem, LLC, which involved a protest of the terms of request for quotations issued by the General Services Administration (GSA), Information Technology Service, for cloud computing services. The GSA had issued the RFQ on May 9, 2011, to establish a SmartBUY blanket purchase agreement of GSA Schedule 70 contract...
holders for cloud computing services. The services would include e-mail as a service. By its terms, the

RFQ did not allow for locating data or data centers in non-U.S. countries other than the designated countries defined by FAR Section 25.003.

The protesters asserted that the limitation on the location of vendors' non-U.S. based data centers was unnecessarily restrictive of competition, that the government community cloud sub-lot specifications were unnecessarily restrictive of competition and exceeded the government's legitimate needs, and that the requirement of common technical requirements was ambiguous and contradictory to the provision of a public cloud solution.

The case ultimately focused on two main issues: the limitation on overseas data centers and the security that could be provided. On the first issue, the GAO's discussion reveals an extraordinary conflict within the US Government. GSA acknowledged that its specification for data center location requirements was a compromise between the security needs of federal agencies (which desired all data to be stored and processed in the United States) - a position that should have trumped any competing priorities - and the advice given by the U.S. Trade Representative's (USTR) office, which had stated that a U.S. data center limitation impermissibly restricted free trade.

Notice that the USTR's position could have the consequence that, in the interest of free trade, U.S. Government data transmitted through this public cloud would needlessly be exposed to high security risks. If that were the choice, and if free trade were a compelling interest in this area, then the US Government should have withdrawn the RFQ and decided against deployment of a public cloud rather than take such risks.

The GAO concluded that GSA's position for data center location limitations was arbitrary (and on this ground ruled for the protesters). The GAO reasoned that "GSA has provided no explanation for why its security concerns would be less acute in relation to data stored or processed in designated [i.e., FAR-prohibited location] countries, which include, for example, Yemen, Somalia, and Afghanistan, versus data stored or processed in non-designated countries, such as Brazil, India, or South Africa."

GAO's argument overlooks the obvious fact that the three countries it gives as examples of FAR-prohibited locations for cloud service centers processing and storing US Government data - Yemen, Somalia and Afghanistan - are well known to be "failed states," incapable of providing basic governmental functions let alone security for a high tech cloud data server farm, and to be countries in which terrorist groups find the lack of security forces a safe haven for organizing actions against U.S. interests. Put differently, what U.S. corporate enterprise would find it acceptable if its prospective public cloud service provider informed it that its data might be stored and processed in Yemen, Somalia, or Afghanistan, when instead it could be stored and processed in countries well-known for their technical capabilities - Brazil, India, or South Africa.

The second issue concerned the RFQ requirement that the service must exclude co-tenant data, or any other third party data, not intended for the Government from being transmitted through a Government network connection. In other words, the Quoter had to provide a cloud specifically limited to "Government clients." The protest therefore turned on whether the government community cloud's restriction on possible co-tenants provided a legitimate benefit to the Government. On this issue, at least, the GAO recognized the overriding importance of the Government's need for security (without explaining how doing so on this issue was consistent with ignoring it on the first issue).

The GAO relied on NIST 800-144 "Guidelines on Security and Privacy in Public Cloud Computing," noting that these NIST Guidelines identified risks inherent in multi-tenancy and co-location of data: "Multi-tenancy in virtual machine-based cloud infrastructures, together with the subtleties in the way physical resources are shared between guest virtual machines, can give rise
to new sources of threat. The most serious is that malicious code can escape the confines of its virtual machine and interfere with the hypervisor or other guest virtual machines.

"The [NIST] report provides several examples of 'attack vectors' possible in a co-tenant environment, beginning with mapping the cloud provider's infrastructure, which researchers have shown to be possible in a cloud providers' service. . . . By mapping the cloud, an attacker can identify the location of a target virtual machine, and create new virtual machines directly co-tenant with the target virtual machine. . . . The attacker can then attempt to bypass or overcome the hypervisor's containment system, which has proven possible. . . . The NIST report also explains several other, more indirect, attacks that can be staged from within a cloud system."

On that basis, the GAO concluded that in light of NIST's substantiation of "unique risks present in multi-tenant cloud environments, the additional layer of security provided by a cloud limited to U.S. government entities - the ability to operate in an environment exclusive of foreign, business, and other potentially hostile entities" presented in GAO's view a meaningful benefit inherent to the government community cloud set forth in the RFQ and thus that there was a meaningful security advantage to the government community cloud deployment model set forth in the RFQ, which justified inclusion of such requirement notwithstanding the protesters' complaint.

The case is thus of importance in showing the apparent disorder within the Government in its push to deploy a public cloud for service of government agencies and the heightened security risks that the cloud presents and that may only be partially mitigated by the requirement for avoidance of co-tenancy. Counsel advising a client considering moving data to the cloud might consider how much more vulnerable their client's enterprise data will be in the likely event that the client will be unable to require the cloud vendor to provide it a similar assurance of no co-tenancy of data with that of any third party.

**Update on the UNCITRAL Working Group on Online Dispute Resolution**
*John Gregory and Hal Burman, Co-Chairs of International Trade Subcommittee*

The UNCITRAL Working Group on Online Dispute Resolution met in mid-November in Vienna. The principal motivation for the ODR project is to improve e-commerce, notably by providing a low-cost form of dispute resolution accessible anywhere in the world. The Working Group is focusing in particular on high-volume, low-value claims that are challenging to resolve under current law with current institutions. The size and volume are more important than whether the claims are B2B or B2C.

The Working Group considered several documents, including a draft text on procedure for ODR and issues involved in creating a global framework for it. All of the documents can be found here. A report of the meeting will be at the same address in a few weeks. The state of play at UNCITRAL and contributions to the US position at the next meeting will be on the agenda of the Winter Working Meeting in San Francisco.

Some people have hoped that ODR could depend on a single consumer-friendly set of legal rules, rather than having to debate the applicable law with each transaction (or having the law impose the law of the consumer's residence, as the EU rule does). A draft common contract law for the EU has been devised recently. Here are the background story and the proposed text (130 pages, though only 80 are legal text). The English and Scottish Law Commissions have analysed this document and issued a report. Our WWM agenda could review whether this kind of proposal is worth pursuing.

**CLC Projects**

**WWM Roundtable with Digital Media and Marketing & Advertising**
Jon Garon and Susan Stephan, Co-Chairs of Digital Media Subcommittee, and Erik Pellon, Chair of Marketing & Advertising Subcommittee

At the Winter Working Meeting, the Digital Media Subcommittee and Marketing & Advertising Subcommittee plan to hold a joint subcommittee roundtable. In addition to legislative updates on the Protect IP Act and SOPA, review of patent laws under the American Invents Act and update on key ongoing litigation (including Golan v. Holder, Viacom v. YouTube, and others), the combined subcommittees will discuss possible new projects for written publications, CLE webinars and other events.

Do You Want to Get Involved or Have an Idea for a Project?

Come to the Winter Working Meeting to learn about other CLC projects in development - or email one of the subcommittee chairs with your ideas.

Other ABA Projects of Note

Trademark Law in China

The People's Republic of China recently proposed changes to its trademark law - details are here. The ABA Intellectual Property Law and International Law sections are planning comments.

Ad Hoc Task Force on Privacy Harms

The Science and Technology Committee of the ABA's Business Law Section is putting together an ad hoc task force on "privacy harms." Its goals include determining what a jurisprudentially sound definition of "Harm" should be relative to an individual's privacy rights and deriving an appropriate definition of non-economic Harm for use by regulatory agencies or courts. If you are interested in joining this effort (or would like more information), please contact John Tomaszewski at johnt@truste.com.

Presentations and Papers of Interest

Cyberspace Feature in Business Law Today

Stay tuned for a cyberspace law mini-theme in the Business Section's electronic magazine, Business Law Today, which should come out later this month. The issue will include these four pieces:

- Professor Jon Garon offers a discussion of two of the most wide-reaching efforts to regulate the Internet to have been introduced in Congress in recent years, in his report on the latest legislative salvos in the content creator - content distributors wars, the recent Pro-IP Act and the Stop Online Piracy Act.
- "Business Interests Under Attack in Cyberspace: Is International Regulation the Right Response?" Hank Judy and David Satola. This piece considers some of the pressures on a fully free and open global network from some of the non-US sources pushing for more international Internet regulation and control. (See more details below.)
- Avoiding Unintended Consequences Under The SEC Staff's 'Cybersecurity Disclosure' Guidance." Prof. Sarah Jane Hughes and Roland Trope. This article explains the SEC's recently-issued guidance concerning corporate data security practices and provides a picture of some of its potentially disruptive unintended consequences.
- "Going Mobile: Are Your Company's Electronic Communications Policies Ready to Travel?" Kathy Porter considers how employers can incorporate employee use of mobile communication devices into their employee electronic communication or internet-usage policies, along with an updated analysis of how some courts have treated employer efforts to access data stored or created on employee devices.
Each of these pieces illustrates how lawyers, regulators, courts, and employers react to cyberspace developments in ways that can have far-reaching, likely unintended, consequences.

Regulating Social Media Use

The November 2011 edition of Business Law Today featured an article covering the NLRB’s evolving stance on regulating employee use of social media. You can read it here.

International Approaches to Internet Regulation

Henry Judy and David Satola, Co-Chairs of Internet Governance Task Force

Committee members Henry Judy and David Satola have co-authored an article to appear in a future edition of Business Law Today. The article explores the debate over the issue of whether there should be state-led international legal instruments to regulate various aspects of the Internet or whether an approach should be followed that favors a more laissez faire, multi-stakeholder approach at the international level. The article concludes that the terms of the debate, as they are widely reported, are misleading and that the fundamental issues involved in the debate turn on the basic principles and values on which any international legal instruments would be based. The article features an analysis of a recent proposal to the United Nations made by China and Russia for a state-led international framework for regulation of Internet cyber-security, permissible content, and intellectual property rights protection.

Online Authentication Challenges

Committee member Tom Smedinghoff recently co-edited an issue of The SciTech Lawyer focusing on "The Challenges of Online Authentication from Evidence to Identity." SciTech section members can access the issue here.

Electronic Contracting

Committee member Juliet Moringiello and her frequent co-author Bill Reynolds of the University of Maryland School of Law presented their work-in-progress, "The Past, Present, and Future of the Law of Electronic Contracting," at a Faculty Workshop at Widener University School of Law on November 1.

Governance of Social Media

On November 11-12, Georgetown University and Michigan State University's Quello Center hosted a two-day conference entitled the "Governance of Social Media Workshop." A large group of academics, policymakers, and representatives from the advocacy community and industry (including representatives of the FTC, Electronic Frontier Foundation, Facebook, and Google) discussed various policy issues raised by social media. The panel presentations emphasized privacy, freedom of expression, and additional topics on the right to pseudonymity and commercial speech. Committee member Jon Garon was one of the thirty participants, speaking on commercial speech and publicity rights issues in digital media. His paper is available here. The conference panels are also available for viewing.

Cloud Computing

Committee member Lisa R. Lifshitz will be chairing and speaking at LEXPERT's first cloud computing conference on December 5, 2011. The conference brochure is here.
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).

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.ababusinesslaw.org

Copyright © 2011