ABA AMERICAN BAR ASSOCIATION Business Law Section

CYBERSPACE LAW COMMITTEE NEWSLETTER

July 2016

Homepage | Committee Roster | Join the Cyberspace Law Committee

In This Issue

Important Dates

Business Law Section Annual Meeting
September 8-10, 2016
Boston, MA

Editorial Board

Message from the Chair

Cyberlawyers,

We work in the midst of a busy summer, building opportunities for your practice development. We are soon to open a new task force - the Current Law Task Force, led by John Black - which will hold meetings every month or two to discuss the breaking news of cyberlaw, Internet, e-commerce and electronic technology, and to write up short blurbs on the news for the rest of us. If you want to participate in the Committee but you can't attend many (or any) of the physical meetings, then this task force is designed for you. The breaking news blurbs may be turned into longer Business Law Today or Business Lawyer Articles if the writer so desires, and the blurbs may lead to topics for webinars or other CLE. Contact me if you are interested in participating, and we will enter you into the new listserv.

The Section Annual Meeting in Boston is two months away and this newsletter contains a description of all of the terrific CLE that our Committee is the primary sponsor for. Next newsletter we will try and include a short discussion of other programs we are co-sponsoring. Our Committee, along with the IP Law Committee, the Corporate Counsel Committee and others, will be sponsoring a Thursday night dinner at Summer Shack, and probably an informal dinner for early arrivers on Wednesday. Stay tuned for more details. As always, the Committee Meeting, subcommittee and task force meetings will all be held on Thursday, so if you can only come for one day, join us on Thursday, September 8.

And despite the heat, it is not too early to consider our Winter Working Meeting at the end of January, 2017. We will be conferring at the recently refurbished U.S. Grant hotel downtown San Diego - minutes from all attractions. Plan to join us. Plan your own presentation if you like.

Our publishing continues apace, and we would love to see your contribution. Our committee has published at least 10 Business Law Today articles already this year (3000 words, no footnotes). The editors have created a special corner of the publication this year for our writing, so we are looking for more articles. Contact me if you have an idea you want to write about. We are still working on the Social Media Law book, the Data Security in Mergers and Acquisitions Book and the Twenty-First Century Payments book, with a couple of others currently on the drawing board. We always need writers and editors.

Ted Claypoole
Chair, Cyberspace Law Committee of the ABA Business Law Section

BLS Annual Meeting - September 8-10

Registration is open for the Business Law Section Annual Meeting in Boston. The Cyberspace Law Committee will have a full day of committee/subcommittee meetings on Thursday, September 8. We will also sponsor CLE programs on:

1. Don't be Spokeo'd: What You Need to Know in Litigating Data Breach Cases (from Breach to Remedies) (Katris)

- This program will cover practical tips regarding what every attorney should know and do when a data breach occurs.
- Includes unique discovery concerns in data breach matters as well as potential remedies and resources for recovery.

2. The Legal Landscape Through a Virtual Reality Lens (Huffman)

- What's up with Virtual Reality technology - development, progress and future outlook of an industry.
- Will cover legal convers of developers, including IP, privacy, speech, impersonation, jurisdiction, data security, and liability concerns.
- The concerns of consumers and advocates also will be addressed.

3. The Government's Role in Your Cyber Incident: Friend, Foe or Both? (McAndrew)

- This program will discuss the various roles that different governmental entities play in a company's cyber life - including establishing standards for, and direct regulation of, organizational cybersecurity and cyber information sharing.
- Provides an understanding of the benefits and costs of interacting with federal law enforcement agencies in the investigation of different types of cyber incidents, using actual case examples to illustrate the issues.
- Highlights key issues in civil and criminal litigation relating to organizational cyber incidents.

4. Securing Your Connected Devices: Plan to Avoid Liability from the Internet of Things (Rothchild)

- Program will provide insight into the Federal Trade Commission's use of its unfairness jurisdiction against manufacturers and users of connected devices with security vulnerabilities.
- Includes a discussion of potential private actions/suits that can be raised, and ways a manufacturers and users of connected devices can reduce their exposure to liability.

5. Director and Officer Liability and Cybersecurity: Questions Every Officer and Director Must Answer (Sarkar)

- Program will discuss the Director and Officer liability exposures as a result of a cyber-incident, including the duties of directors and officers have with respect to cyber security and how to address their related fiduciary responsibilities.

6. Blockchain for Business: Emerging Legal Issues Associated With Using Distributed Ledger Technology in a B2B Environment (Middlebrook/Hughes)

- Program will discuss what distributed ledger technology ("DLT") is and how it is being integrated into business models and processes.
- Includes a description of the roles and responsibilities of entities involved in DLT projects as well as the key legal issues business lawyers need to assess when reviewing DLT projects.

The Early Bird discount of $100 ends on July 15, so secure your registration now. Make sure to reserve your hotel too before the room blocks sell out. As this newsletter goes to press, the ABA has not yet posted all of the committee dinners for purchase. We will let you know as soon as they are available so that you can add the Cyberspace Law Committee's dinner at Summer Shack-a fun seafood joint run by Jasper White, a James Beard award-winning chef who believes great food doesn't need to be "haute"! We look forward to seeing you in Boston.

DHS Proposes Collecting Social Media Account Information

By Steve Middlebrook
Co-chair, Financial Services and Payments Subcommittee

The Department of Homeland Security is proposing to collect social media account information from people crossing the border. In a very short, very cryptic, Federal Register announcement, U.S. Customs and Border Protection (CBP) has given notice that it intends to modify several forms which foreigners are required to fill out before entering the country to collect information on travelers' social media presence. 81 Fed. Reg. 40892 (June 23, 2016). The proposal is disturbing because while it significantly impacts expressive activity, the agency's proposal, barely a page and half long, fails to address a number of legal issues, including implications for the First Amendment.

CBP plans to modify the forms to state "Please enter information associated with your online presence - Provider/Platform - Social media identifier." There is no explanation as to what "online presence" means or what providers and platforms this requirement covers. CBP says this "will be an optional data field to request social media identifiers to be used for vetting purposes, as well as applicant contact information." Nothing on the forms, however, indicates that providing social media information is optional and it seems unlikely that a traveler would think the collection is voluntary. According to CBP, they estimate that 32 million people a year will be required to fill out these forms.

Why does CBP want this information? Their justification is contained in a single sentence: "Collecting social media data will enhance the existing investigative process and provide DHS greater clarity and visibility to possible nefarious activity and connections by providing an additional tool set which analysts and investigators may use to better analyze and investigate the case." Given that this data collection directly impacts expressive activity, one would expect more than a single sentence justification for the government's actions. Vetting visitors based upon their speech activities raises significant First Amendment questions which the agency does not even appear to have considered.

The proposal also does not address a number of obvious questions, such as where and how this information will be stored, who will have access to the information and how it will be used. Of special concern, given that the population targeted by this information collection is foreign visitors to the United States, is whether Homeland Security plans to divulge this information to travelers' home countries. Sharing information on social media participation with more repressive governments could result in harassment or incarceration of political dissents, ethnic and religious minorities, and other disfavored people. Even if the data isn't going to be intentionally shared with other governments, how does CBP propose to protect this sensitive information from foreign sovereign hackers?

Cyberspace committee members interested in this issue may review the Federal Register notice at https://www.gpo.gov/fdsys/pkg/FR-2016-06-23/pdf/2016-14848.pdf. The comment deadline is August 22, 2016. If wish to express your views on this proposal, you'll need to get out pen and paper because CBP is not accepting comments over the internet or by email or social media.

DC Circuit Finds for FCC in Net Neutrality Decision

By Stuart Call
2L, George Washington University Law School

On June 14, 2016, in United States Telecom Ass'n v. FCC, the DC Circuit Court of Appeals decided in a 2-1 decision that the FCC properly classified fixed and mobile broadband service providers as offering telecommunications services in its 2015 Open Internet Order, and that the classification was consistent with 47 U.S.C. § 153(51), the 1996 Telecommunications Act, which requires that providers of telecommunications services (as opposed to information services) are to be regulated as common carriers.

The FCC's 2015 Open Internet Order has three main bright line rules prohibiting blocking, throttling, and paid prioritization. Additionally, the common carrier classification allows the FCC to impose stricter privacy standards on broadband providers. This came after concern that broadband internet providers would discriminate against certain types of online traffic, favoring traffic directed toward their own content, at the disadvantage of edge content providers such as Netflix, YouTube, etc. This is not the first time this concern has been raised. In 2008, Comcast was found to have throttled down peer-to-peer traffic on its network.

The DC Court of Appeals decision hinges largely on the statutory interpretation of what internet providers are offering - information services or telecommunication services. The 1996 Telecommunications Act defines a telecommunications service as offering for a fee, the "transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." See 47 USC § 153(50). The Act defines an information service as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service." See 47 USC § 153(24).

In the case, the United States Telecom Association argued that 1) the FCC improperly classified fixed and mobile broadband as a telecommunications service, 2) the FCC did not give proper notice during the notice of proposed rule making process, and 3) the FCC acted arbitrarily and capriciously in its classification of fixed and mobile broadband as a telecommunications service.

The Court concluded:

1) the FCC properly classified broadband as a telecommunications service, because its determination that broadband providers offer stand alone telecommunication services that function as "transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received", 47 USC § 153(50), was consistent the 1996 Telecommunications Act and with the Supreme Court's decision in Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005) (holding that classification of broadband depends on if its information services and telecommunication services offered are functionally integrated or separated, as well as the consumer perception of that integration);

2) the FCC followed proper notice of proposed rule making procedures in its promulgation of the Open Internet Order by giving extensive background and support to its order and by allowing a large comment period; and

3) the FCC did not act arbitrarily or capriciously in its reclassification because its decision, made on reliance of the virtuous cycle theory for internet growth and innovation, was rational and reasonable, and the FCC had properly considered the impacts of its order on consumers and internet providers.

The US Telecom Association, along with others, argue that the classification is unnecessary and will stifle infrastructure and other growth and investments in the broadband and internet provider industry, potentially increasing costs for consumers.

Although the FCC has at this point decided to forbear from requiring local-loop unbundling, this classification opens the door for this requirement in the future, which some argue will increase competition among providers.

Don't Post That Rhino Pic!

By Lisa R. Lifshitz
Torkin Manes LLP

"Please don't post any of your rhino pictures on social media!"

This comment, given by a fellow tourist and echoed by one of the trackers from Save the Rhino Trust after spending an exhilarating morning tracking a black rhino in Damaraland, Namibia, reminded me how technology can be a force for both good and evil. Nowhere is this more evident in the fight against rhino poaching in Africa, where it is clear that technology is a double-edged sword for wildlife.

Presently, rhinos of all types are some of the most endangered animals in Africa. Since 2007, rhino poaching has increased 9,000 per cent. Rhinos are being slaughtered mercilessly due to the demand for their horns in Vietnam and China.

Despite the lack of any scientific data, pulverized rhino horn is believed to cure strokes, convulsions, and fevers, among other ailments. A single rhino horn can fetch more than $250,0000 on the black market.

With these kind of financial incentives, poachers scour social media looking for leads on where to find endangered species. Images posted on Facebook, Twitter, and Instagram can betray details of an animal's location. As Mike Hower noted in his article on the dark side of digital technology, seemingly innocuous social media apps such as Instagram have become useful tools for tech-savvy poachers.

Read more...

Committee Doings

From the Mobile and Connected Devices Subcommittee
Co-chairs John Rothchild and Richard Balough

The Mobile and Connected Devices Subcommittee is busy planning a CLE program that it will present at the Annual Meeting in Boston, titled "Securing Your Connected Devices: Plan to Avoid Liability from the Internet of Things." Here's a brief description of it: "The number of consumer-facing devices that are connected to the Internet, known as the Internet of Things, is increasing exponentially. These devices often have weak security protections and are vulnerable to unauthorized access by hackers. This program will provide information about the types of legal claims that may be brought against entities that either manufacture or deploy connected devices with inadequate security against unauthorized access." We have had discussions with several potential program participants, and we are hoping to have a participant from the FTC, a lawyer with experience bringing lawsuits against manufacturers of devices with security vulnerabilities, and a person who can discuss best practices for securing connected devices.

From the Enterprise Technology Subcommittee
Co-chairs Candace Jones and Cheryl Burtzel

The Enterprise Technology Subcommittee continues its work on the project ***Contracting with Vendors for Information Security and Resiliency***. The project has benefited from participation by ABA members in diverse roles, including in-house counsel for companies from a variety of industries, federal agencies, state and local government, non-profits, and trade associations as well as private practitioners. Participants have included lawyers with experience in representing entities procuring enterprise technology solutions as well as vendors. We appreciate the energetic exchanges and insights provided by these participants.

These calls occur every two weeks from **12:00 noon Eastern Time on the first and third Thursday of each month**. Our next call is planned for **Thursday, July 21, 2016 at 12:00 Noon Eastern**.

The purpose of the calls is to have structured discussion about the particular topic for the call agenda. An agenda for each call will be distributed the week of the call to those who sign up with Cheryl Burtzel or Candace Jones. We welcome volunteers to serve as "reporters" for the workshop calls and author/editors of the materials we develop based on those calls.

We have distributed a discussion draft of a checklist to help address the issues surrounding information security provisions in vendor contracts through a series of workshop conference calls. The project also will begin soliciting sample contract clauses from participants soon. We welcome volunteers to serve as "reporters" for the workshop calls and author/editors of the other materials we plan develop based on those calls.

Please let us know if you are interested in participating in one of those roles or otherwise contributing to the project.

Member News

The Uniform Law Commission will have the first reading of the Uniform Regulation of Virtual Currency Business Act on July 13th. Steve Middlebrook, the ABA Advisor, will be present to answer questions from the membership. Sarah Jane Hughes is the reporter for the project.

Juliet Moringiello has been appointed to the Uniform Law Commission study committee on Identity Management in Electronic Commerce. Longtime Cyberspace Committee member Pat Fry is the Vice-Chair of the study committee.

Upcoming Programs of Interest

Theft or Art?: Protecting Pictures and Images Online
July 7, 2016
Format: Webinar

Digital Assets: Estate Planning, Conflicts in Law, and Advising Clients on Changing Rules
July 12, 2016
Format: Webinar

The Federalization of Trade Secrets
July 12, 2016
Format: Webinar

FinTech-Introduction and Overview
July 13, 2016
Format: Webinar

Recent Developments in FTC and CFPB Data Security Enforcement
July 19, 2016
Format: Webinar

The Rise of the Machines: Artificial Intelligence and the Future of Law Practice
July 20, 2016
Format: Webinar

A Note from the Editor

In addition to reporting on the committee's work and what its members are up to, we'd like the newsletter to include articles on topics of interest to members. Articles should be 250-500 words, timely, and original content not already published elsewhere (including on your firm's website). To submit an article or ask questions, please contact the editor, Lois Mermelstein.

American Bar Association | 321 N Clark, Chicago, IL 60654-7598 | 800-285-2221 | 312-988-5522

Don’t Post That Rhino Pic!

By Lisa R. Lifshitz
Torkin Manes LLP

“Please don’t post any of your rhino pictures on social media!”

This comment, given by a fellow tourist and echoed by one of the trackers from Save the Rhino Trust after spending an exhilarating morning tracking a black rhino in Damaraland, Namibia, reminded me how technology can be a force for both good and evil. Nowhere is this more evident in the fight against rhino poaching in Africa, where it is clear that technology is a double-edged sword for wildlife.

Presently, rhinos of all types are some of the most endangered animals in Africa. Since 2007, rhino poaching has increased 9,000 per cent. Rhinos are being slaughtered mercilessly due to the demand for their horns in Vietnam and China.

Despite the lack of any scientific data, pulverized rhino horn is believed to cure strokes, convulsions, and fevers, among other ailments. A single rhino horn can fetch more than $250,0000 on the black market.

With these kind of financial incentives, poachers scour social media looking for leads on where to find endangered species. Images posted on Facebook, Twitter, and Instagram can betray details of an animal’s location. As Mike Hower noted in his article on the dark side of digital technology, seemingly innocuous social media apps such as Instagram have become useful tools for tech-savvy poachers.

Apparently, in South Africa, poachers have gone so far as to send in young couples with GPS-enabled smartphones to photograph endangered rhinos. The exact GPS co-ordinates are attached to the picture, which allows poachers to come in after dark and track the animal. Clueless tourists thus become unwitting accomplices to poaching.

Conservationists have posted signs in wildlife reserves reminding people to turn off the geotag function and not disclose where the photo was taken. Plugging the longitude and latitude into Google Maps, for example, allows one to discover the exact spot where the photo was shot, give or take a few metres.

Amazingly, poachers can even identify markers in the background of photos, such as a particular grove of trees or a mountain peak. As some rhinos are sedentary and can remain in a general area for days at a stretch, the risk increases exponentially.

Would-be poachers or informants can then send a photo with a location tag to anyone or return to the spot later to seek out the rhino. Poachers use helicopters so they can cover large distances in a short period of time to hunt down the animal quickly.

Paranoia? In South Africa’s Hluhluwe-Imfolozi Park, two men killed a pair of white rhinos and were later arrested. In India, poachers killed a pair of one-horned rhinos in Kaziranga National Park.

In reaction, officials in South Africa have become more vigilant about rhino tourism, documenting the names and visits of tourists. Cellphones are forbidden on some safari vehicles. Desert Rhino Camp, where I stayed, did not have any Wi-Fi access, for which I was glad if it meant helping to preserve, even a little, the safety of the rhinos.

Social media is being used in other twisted ways. In March, Traffic, a strategic alliance of the World Wildlife Fund and the International Union for Conservation of Nature, issued a report that confirmed social media sites are increasingly being used in Asia as platforms for the illegal trade in a range of threatened species such as orangutan and sun bears.

“Traders are clearly moving to non-conventional methods of sale such as utilizing online portals and social media in order to evade detection, reach a broader audience, and increase transaction efficiency and convenience,” Traffic said in a report released to coincide with World Wildlife Day.

Growing numbers of traders are using closed groups on Facebook and password-protected online forums to reach Asian customers. Traffic said in one month in China last year, thousands of ivory products, 77 whole rhino horns, and large numbers of endangered birds were found advertised for sale on sites such as QQ and WeChat, which are popular in China, using code words for the various products.

On the positive side, social media is also being used to fight poachers. In cases that range from China and Africa to the United States, poachers who have bragged on social media have found themselves nabbed for their crimes by a combination of amateur sleuths and law enforcement worldwide.

Additionally, various new technologies are being tested and used to combat wildlife crime. Drones, satellite imagery, predictive analysis, DNA analysis, hidden cameras, GPS location devices, and apps are all being implemented to try and predict, locate, track, and catch suspected poachers.

Drones in particular have really taken off (pun intended) in attracting funding for conservation efforts. In 2012, Google gave US$5 million to the World Wildlife Fund to purchase conservation drones to fly over parts of Africa and Asia in an attempt to help monitor and catch wildlife poachers. In March 2014, the Howard G. Buffett Foundation announced a 255-million rand (Cdn$22 million) donation for a three-year initiative in partnership with Nature Conservation Trust, South African National Parks, and a South African public benefit organization to combat poaching in Kruger National Park and test new anti-poaching technology.

In March, the Lindbergh Foundation announced the launch of the Air Shepherd program in South Africa, using military-style computer analytics to identify poaching hot spots, and then send silent drones equipped with night vision to track down poachers. In partnership with the University of Maryland Institute for Advanced Computer Studies, they use algorithms to predict when and where the poaching will take place. Rangers are then pre-deployed to intercept poachers before the rhino is killed.

Can drones be used successfully to help combat rhino poaching? As noted by Save the Rhino in its excellent article on Rhinos and Drones, drones definitely have limitations as rhino-protection tools in the long term.

The technological limitations are myriad — they have a limited battery life, range must be within line-of-sight of the operator, and any malfunction can lead to an expensive crash. The payload (thermal-imaging equipment, etc.) can make them heavy, and gusty winds, hilly terrain, or other unfavourable conditions can make them difficult to operate.

Most importantly perhaps, unmanned drones still require skilled operators. If the operator has not received sufficient training, the capabilities will not be fully utilized. Worse, drone operators have allegedly been bribed to give out sensitive rhino location details to poachers.

Taking a different approach from using drones, Cisco and Dimension Data teamed up this year to deploy a number of different crime-fighting technologies in an unnamed South African reserve. Their initiative focuses on monitoring and tracking individuals as they enter the gates of the reserve and until they leave.

Dimension Data worked with Cisco to collect various bits of information about the game rangers, security personnel, tech, and control centre teams. They then created a secure Reserve Area Network and installed Wi-Fi hotspots at key points around the reserve. The second phase involves CCTV, drones sporting infrared cameras, thermal imaging, vehicle-tracking IoT sensors and seismic IoT sensors on a secure intelligent network.

All of this technology is operated on the site as a managed service and utilizes the cloud for data analytics and backup. Suspicious activities/crimes are supposed to be recorded and stopped as they happen. Depending on the results, the technology will be expanded to other reserves in Africa.

Many believe a low-tech solution still works better. In fact, tracker dogs, working alongside their human handlers, are responsible for more than 70 per cent of arrests of suspected poachers in Kruger. “Killer,” a Belgian Malinois dog, has led to 115 arrests over the past four years.

While drones are still being used, the goals now are more modest. “They’re not the game-changer they have been portrayed to be,” says Julian Rademeyer, author of *Killing for Profit*, a book about the illegal rhino-horn trade.

In Namibia, SRT is currently focusing on increasing its field patrolling and monitoring (using a combination of vehicles and increased air and foot patrols), and working closely with their partners and with local communities to engage them in helping to save the rhino.

Since locals know where the rhinos are, more or less, and know how to find them, poachers will often send a middleman to bribe a local to go shoot the rhinos and hack off the horn for them. SRT critically seeks to engage black-rhino host communities to improve understanding of the long-term value to them of the rhinos, making them partners in rhino conservation.

This includes obtaining more local rhino rangers and liaising and engaging with schools and communities in town and in areas surrounding the rhino range. It’s a decidedly more low-tech approach that may be more useful than drones in protecting the rhino in the future.

However, the only way to really protect these magnificent animals will be to persuade would-be buyers in Asia to stop using their horns, which, unfortunately so far, technology — and social media — has not yet been able to successfully do.

For more information about the excellent work being done by Save the Rhino Trust (Namibia), visit its web site.