State Bar of Michigan

Michigan IT Lawyer

A Publication of the State Bar of Michigan Information Technology Law Section

http://www.michbar.org/it

Table of Contents

October 2013 ▪ Vol. 30, Issue 5

- Bits and Bytes from the Section 1
- Information Technology Law Section, State Bar of Michigan Mission Statement.....3
- Flirting with Disaster: CDA 230's Overbroad Protection of Dating Websites and the Unenforceability of Reputational Assertions 4
- 2014 Edward F. Langs Writing Award ..22
- The State of Information Technology Law—2013 23

Michigan IT Lawyer is published every other month. Previously published issues of the *Michigan IT Lawyer*, and its predecessor the *Michigan Computer Lawyer*, are available at http://www.michbar.org/it/newsletters.cfm. If you have an article you would like considered for publication, send a copy to:

Michael Gallo
2700 Renshaw Drive
Troy, Michigan 48085
e-mail: michael@gallo.us.com

Bits and Bytes from the Section

By Michael Gallo, 2013-2014 IT Law Section Chairperson-Elect

Welcome to autumn!

During September, the IT Law Section sponsored the 6th Annual Information Technology Law Seminar, presented in cooperation with *ICLE* (The Institute of Continuing Legal Education). This year's seminar was titled '**Core Legal Issues in a High-Tech Business World**', and included an exhibit by *Spectrum Computer Forensics and Risk Management LLC*, www.spectrumforensics.com. Of course, thanks go to the generous event sponsors, which included:

- *Bejin, VanOphem & Bieneman PLC*, www.bvbip.com
- *Brooks Kushman PC*, www.brookskushman.com
- *Dykema*, www.dykema.com
- *Rader, Fishman & Grauer*, www.raderfishman.com

The seminar was moderated by **Ronald S. Nixon**, *Kemp Klein Law Firm*, and included six presentations:

Designing Privacy Notices for Mobile Devices and Applications, in which **Robert S. Gurwin**, *AOL Inc.*, presented on topics that included:

- Reviewing regulatory and self-regulatory issues surrounding privacy notices
- Ensuring compliance across digital media
- Composing privacy notices that are easy to comprehend and meet legal requirements
- Legal and design issues in mobile privacy notices
- Practice tips for working with mobile app developers

Continued on next page

Bits and Bytes . . .

Continued from page 1

Basics of Computer IP Protection, offered by **Susan M. Kornfield**, *Bodman PLC*, which discussed:

- The IP toolbox: when a client develops new technology
- The contract: tips and traps in IP clauses
- The authorities: involving police and the DOJ in technology protection

Maintaining Privacy Policies and Responding to Security Breaches, a topical presentation by **Keith A. Cheresko**, *Privacy Associates International*, which presented:

- Overview of privacy notices
- Cyber-attacks against law firms
- Practical approaches to protecting data

International Privacy Update, given by **Robert L. Rothman**, *Privacy Associates International*, which covered issues such as:

- Basics of cross-border transfers of personal information
- Cross-border discovery issues
- Cross-border mergers and acquisitions
- Proposed EU Regulation

E-Discovery Almost a Decade after Sedona, delivered by **Leigh C. Taggart**, *Rader Fishman & Grauer PLLC*, and included concerns such as:

- The current key topics in e-discovery
- Spoliation – what is and what isn't?
- The (near) future of e-discovery

Ten Tips for Navigating Cloud Computing by **H. Ward Classen**, *Computer Sciences Corporation*, and included material about:

- What are a customer's obligations regarding personal information it uploads to the cloud?
- Why should a customer know where its data will be processed and stored, and by whom?
- What are the purposes of service levels and how should service level provisions be evaluated?
- When should a party be permitted to terminate a cloud computing agreement?
- How should a customer evaluate a cloud service provider's force majeure clause?

- What implementation services are customary in cloud computing transactions?

In addition to the presentations listed above, the IT Law Section's annual Section Meeting took place, was followed by a Section Council meeting, and the day closed with a complimentary networking reception!

During the Section's Annual Meeting, the following Section members were unanimously voted to the Section Council for a three year term:

- Susanna C. Brennan
- William Henry Hartwell
- Donna K. Malonee
- Carla M. Perrota
- Robert L. Rothman
- Clara Lauren Seymour
- Nathan William Steed
- David R. Syrowik

During the Section Council meeting, **Ronald S. Nixon** was named Chairperson for 2013/2014, and other officers named include **Michael Gallo**, Chairperson-Elect, and **Susanna C. Brennan**, Secretary.

Special thanks go out to **Karl Hochkammer**, who served as the Section's 2012/2013 Chairperson, and now transitions to become an Ex-Officio member of the Council. Though moving out of an officer role, the Section and Council look forward to Mr. Hochkammer's involvement and participation for many years to come!

REMINDER: On LinkedIn, the group 'IT Law Section of the State Bar of Michigan' has about 170 members. If you are not a member, please join the group and use this resource to connect with your peers by posting to 'Discussions' or 'Jobs', by initiating a 'Poll' or by requesting creation of a 'Subgroup'. Your participation is welcome and desired!

Regards,

Michael Gallo

2013-2014 Section Chairperson-Elect

Information Technology Law Section, State Bar of Michigan Mission Statement

The purposes of the Section are to review, comment upon, and appraise members of the State Bar of Michigan and others of developments in the law relating to information technology, including:

(a.) the protection of intellectual and other proprietary rights;

(b.) sale, leasing, distribution, provision, and use of, hardware, software, services, and technology, including computer and data processing equipment, computer software and services, games and gaming, information processing, programming, and computer networks;

(c.) electronic commerce

(d.) electronic implementation of governmental and other non-commercial functions;

(e.) the Internet and other networks; and

(f.) associated contract and tort liabilities, and related civil and criminal legal consequences.

The Information Technology Law Section's bylaws can be viewed by accessing http://www.michbar.org/it/councilinfo.cfm and clicking the 'Bylaws' link.

The *Michigan IT Lawyer* is pleased to present "Flirting with Disaster: CDA 230's Overbroad Protection of Dating Websites and the Unenforceability of Reputational Assertions" by Mattias J. Kaseorg, a 2013 *magna cum laude* graduate of Washington and Lee University School of Law, who received the *Order of the Coif*.

The statements made and opinions expressed in this essay are strictly those of the author, and not the State Bar of Michigan or the Information Technology Law Section. Comments regarding this article can be forwarded to the Michigan IT Lawyer, care of *michael@gallo.us.com*. Enjoy!

Flirting with Disaster:

CDA 230's Overbroad Protection of Dating Websites and the Unenforceability of Reputational Assertions

By Matthias J. Kaseorg

"Dating is a battleground filled with deception and infidelity."[1]

"When virtual reality gets cheaper than dating, society is doomed."[2]

Matthias J. Kaseorg

Introduction

Welcome to the jungle. The world of online dating is a dangerous and unpredictable one. Users seeking love may find themselves in a veritable menagerie of falsified profiles, misleading websites, conniving con-artists, violent criminals, and perhaps a soulmate or two. Despite the Internet's murky waters and associated dangers, online dating has steadily grown as an alternative to traditional forms of courtship.[3]

Since Congress passed Section 230 of the Communication Decency Act (CDA 230) in 1996,[4] courts have systematically expanded the breadth and scope of CDA 230's liability shield, which prohibits courts from treating an interactive computer service as "the publisher or speaker" of its users' content.[5] This Note specifically examines CDA 230 in the context of dating websites, but many of the same principles apply to a broad range of Online Service Providers (OSPs).

This Note argues that courts twisted CDA 230 to grant immunity for a far broader subset of conduct than Congress originally intended,[6] and, in doing so, undermined CDA 230's own stated purpose.[7] Some critics have taken notice of CDA 230's broad liability shield, but have improperly focused on dating violence as the problem and negligence liability as the solution.[8] This Note instead focuses on dating websites' reputational assertions—assertions of facts, user characteristics, or website policies.[9] This Note argues that dating users, dating websites, and the broader Internet community suffer as a result of dating websites enjoying immunity from false reputational representations,[10] and that contract and fraud liability are the solution.[11] This Note provides several examples of unregulated reputational assertions—most notably infamous infidelity-facilitation website AshleyMadison.[12]

This Note suggests that CDA 230 should be reformed in two fundamental ways. First, courts should adopt a uniform jurisprudence that does not shield dating websites from liability for certain kinds of conduct entirely within their control.[13] Second, the legislature should pass an amendment to CDA 230 that adopts a safe-harbor provision to protect dating websites from speech-chilling liability for user conduct outside of their control.[14]

CDA 230 and Associated Jurisprudence

In 1995, *Stratton Oakmont, Inc. v. Prodigy Services Co.*[15] held that an OSP could be held liable for the speech content of its users.[16] In response to the *Stratton* decision, Congress

HOME BACK NEXT

passed CDA 230 in 1996.[17] CDA 230 immunizes OSPs from being "treated as the publisher or speaker" of third-party content.[18] On its face, CDA 230 immunizes a website from tort liability when a user posts actionable content, because holding the website liable for the user's conduct would require treating the OSP, rather than the user, as the content publisher.[19] Courts extended CDA 230's liability immunization much further, however.

Current Key Jurisprudence

Zeran v. America Online, Inc.[20] in 1997 was the first major court decision to interpret CDA 230. *Zeran* extended CDA 230 immunity beyond libel to other kinds of tort actions.[21] In *Zeran*, an anonymous individual posted Kenneth Zeran's personal phone number on America Online's forum as a prank.[22] As a result, Mr. Zeran received several abusive phone calls and death threats.[23] The court applied CDA 230 to immunize America Online from state negligence liability for failure to take down the message, even though Mr. Zeran had notified America Online of the objectionable content.[24]

In 2007, *Doe v. SexSearch.com* extended CDA 230 immunity to protect OSPs from contract claims as well.[25] SexSearch.com allows adults to create profiles and send messages to other adults who they wish to have sexual encounters with.[26] SexSearch.com asserted on its website that all members were at least eighteen years old, and that SexSearch.com would bar any minors from accessing the website.[27] The plaintiff, an adult male, made a profile on the website and began communicating with a fourteen-year-old girl who had misrepresented that she was at least eighteen years old.[28] The two individuals had a sexual encounter and the man was arrested for unlawful sexual conduct with a minor.[29] The man sued SexSearch.com for, among other things, publishing a minor's profile on its website and failing to properly police the website in violation of SexSearch.com's explicit promises.[30] The court refused to hold SexSearch.com liable for failing to keep its stated promises; to hold SexSearch.com liable would require the court to treat SexSearch.com as the publisher of the girl's profile, which would contravene CDA 230's express provisions.[31]

In 2008, *Jane Doe v. MySpace*[32] also broadly interpreted CDA 230's liability protection. MySpace is a social media website which facilitates user interaction by permitting users to create profiles, post information, and send messages to one another.[33] In *Jane Doe v. MySpace*, thirteen-year-old Jane Doe registered a profile on MySpace and misrepresented that she was eighteen years old.[34] Jane Doe, by misrepresenting her age, was able use MySpace.com's full functionality, which included the ability to make her profile publically available—a feature that MySpace denies to individuals younger than eighteen years old.[35] Jane Doe conversed with, and arranged a meeting with, a nineteen-year-old boy who she met on the website.[36] The boy then sexually assaulted Jane Doe.[37] Jane Doe and her family sued MySpace for negligently failing to verify Jane Doe's age before making her profile publically available.[38] The court held that CDA 230 immunized MySpace from negligence liability because Jane Doe failed to allege that MySpace was responsible for Jane Doe's *content* on the website.[39]

Background

A (Brief) History of Dating Services

The advent of flirtatious romantic relationships is relatively recent in our country's history. [40] In the past, the realities of a work-intensive life, coupled with a patriarchal philosophy that women were subservient beings who provided household services and required men for survival, led to a very practical approach to marriages.[41]

As people began to settle in great numbers into populated cities in the 20th century, formal courtship became the new norm for romantic relationships.[42] With need came entrepreneurism, and dating services began to appear.[43] Television legitimized the matchmaking experience with shows such as the 1950s' "Blind Date."[44]

In the 1990s, computers fundamentally changed the dating landscape.[45] Today, social networking has become integral in facilitating romantic relationships—through casual social websites such as Facebook or Google+ or through dedicated dating websites.[46]

Reputational Assertions

Modern dating websites are very profitable endeavors and are often owned by large corporate entities.[47] As such, they have many of the features one might expect in a standard business website.[48] Most relevantly, dating websites contain various assertions about reputational characteristics of the dating service and client base. There are four different "tiers" of reputational assertions often found on dating websites.

First, some content is purely user-generated. Users may generate and post information about themselves or others, or make a selection indicating that they possess one characteristic or another.[49] The dating website then aggregates this information in a search index, but does not have control over what a user decides to post.[50] Thus, although the dating website may aggregate the information in a searchable form, users make all of their own representations.

Second, a dating website may include descriptions of what audience it intend to cater to.[51] This is analogous to an establishment serving alcoholic beverages describing itself as a "biker bar," a clothing store describing itself as a "women's boutique," or a baseball stadium hosting a "kids' night." People may generally expect patrons with the advertised characteristic to frequent the establishment. People would not reasonably expect the establishment to exclusively allow patrons with the particular characteristic and deny all other patrons access, however, unless the establishment explicitly stated otherwise.

Third, a dating website may go beyond merely describing its intended audience, and instead assert that a specific portion of its patrons have particular characteristics.[52] This is analogous to a foreign-language housing community asserting that "sixty percent of residents are fluent in Spanish." A would-be homeowner in this fictional community would probably expect some degree of accuracy with regards to the community's claim, and seek redress if it turned out that very few residents spoke Spanish with any fluency.

Fourth, a dating website may affirmatively assert that it will take specified actions to verify that member characteristics fall within its guidelines.[53] This is analogous to an establishment promising that it will permit "only women" to attend a particular social gathering. Alternatively, a dating website may assert that the potential user will necessarily gain some benefit from using the dating website.[54] This is how we traditionally view contracts—as a bargained-for exchange of one thing of value for another. This is analogous to a bar promising that patrons will walk out with a free T-shirt if they pay the attendance fee on a particular night. Dating websites' affirmative promises are often (if not always) tied up with user conduct, as we saw in *SexSearch*.[55]

Summary of Current Legal Standard and Possible Plaintiff Theories

When user content is at issue, courts construe CDA 230 broadly to protect OSPs.[56] CDA 230 grants full immunity to OSPs for content provided by users, regardless of how OSPs select or edit the displayed user content.[57] Further, courts will not hold OSPs liable for failing to deny users communication privileges or content access.[58]

In *Julie Doe II v. MySpace*, the Fourth Circuit created a three-part test for CDA 230 immunity: (1) the OSP must be an interactive computer service provider; (2) the OSP must not be an information content provider with respect to the information central to the cause of action; and (3) the information leading to the plaintiff's cause of action must have originated from a third-party user.[59] This full immunity extends to all civil claims,[60] including ancillary claims arising from user content.[61] Although CDA 230 lists some exceptions, they are not at issue here.[62]

Content Provider / Content Host Distinction

CDA 230 expressly applies only when information is "provided by another information content provider."[63] Courts have used this statutory limitation to create a distinction in legal status under CDA 230 between content providers and content hosts.

In *Julie Doe II v. MySpace*, the court dismissed the idea that MySpace.com user profiles were MySpace's own content, and instead found that MySpace was a content host for its users' content.[64] The court therefore held MySpace.com, as a content host, immune from liability for its users' actions.[65] Similarly, in the housing context, *Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc.*[66] held that a message board host, which allowed users to post their own content into various self-selected topic-differentiated sub-boards, was not liable for the racially-discriminatory housing advertisements posted by users.[67] The court concluded that "[a]n interactive computer service 'causes' postings only in the sense of providing a place where people can post."[68] In *Fair Hous. Council v. Roommates.com, LLC*,[69] however, the court held that Roommates.com was a content provider and liable for discriminatory housing practices when it created a "check-box" housing form that allowed would-be-renters to search for—and choose whether to sublet to—prospective roommates by gender, sexual orientation, and whether they are bringing children.[70]

Current jurisprudence, thus, suggests that a plaintiff may successfully circumvent a dating website's CDA 230 immunity if she successfully argues that the dating website was in some way an active content provider rather than merely a passive content host. The differentiating factor between *Craigslist* and *Roommates* appears to be the level of creative control that the OSP retains over the final content that is ultimately displayed. The "hands-off" approach of *Craigslist* invokes CDA 230 protection, while a *Roommates*-style "pigeonhole" approach that forces users to choose from preselected options does not invoke CDA 230 protection.

Dating websites appear to have both hands-off elements and pigeonhole elements.[71] Even if a dating website is an information host with respect to some user-generated information, it may still be held liable for claims arising out of self-generated information; it is possible for an OSP to have legal statuses of both content host and content provider concurrently.[72]

It is important to reiterate that CDA 230 is not particularly concerned with the level of editorial control that the OSP retains over user content.[73] This comports with CDA 230's policy rationale of encouraging OSPs to take appropriate care to moderate their services without fear of legal retribution for their good-faith efforts.[74] Intuitively, it may seem rational to impose greater liability on OSPs that have greater ability to control user content and, therefore, to prevent legal harm. This policy rational underlies the tort principle of respondeat superior—courts impose greater liability on the party with the ability to control.[75] But ironically, this very liability would incentivize OSPs to adopt the legally-safer ostrich position by firing all moderators and letting users run rampant and free.[76]

Contract Liability

The first potential source of liability for a content host—rather than a content provider—stems from contract law. In general, Internet contract law is treated much the same as traditional contract law.[77]

When users sign up for a dating website such as Match.com, they enter into a bargained-for exchange. Online dating websites are huge money-makers.[78] Users generate revenue for the dating website, through subscription fees and advertisements, and they expect something in return.[79] There are three potential sources for this "something in return." First, the user expects some basic level of dating "service."[80] Second, the dating website provides reputational assertions and affirmative promises throughout the homepage, the small text at the bottom of the page, and other website pages.[81] Third, the dating website provides additional information, promises, assertions, and disclaimers in its Terms of Service, which the user must accept when he or she joins the dating website.[82]

Under current Internet contract jurisprudence, the direct information contained within the terms of service is part of the contract for sale of dating services.[83] A contract theory of liability would argue, furthermore, that the visible assertions and promises on the dating website should also be included.[84] This Note does not address the broad contours of Internet contracting law and all its contingencies.

Current CDA 230 jurisprudence, however, seems to bar even an inquiry into contract validity when user conduct is at issue. The aforementioned *SexSearch* line of reasoning suggests that OSPs are immune from contractual liability when the reason for a breach of contract centers on user conduct.[85] Another line of reasoning suggests that CDA 230 might not protect OSPs against contract liability in certain circumstances. In *Barnes v. Yahoo*,[86] the Ninth Circuit held that a manifestation of intent, in a contractual context, "generates a legal duty distinct from the conduct at hand."[87] Thus, CDA 230 may not bar true contract claims, because the OSP's legal duty exists independently of the user's conduct.[88]

An important threshold question is "what manifestation of intent qualifies as a legally-binding contract?" *Barnes* did not ultimately reach the answer to this question.[89] *Barnes* did state, however, that "a general monitoring policy, or even an attempt to help a particular person, on the part of an interactive computer service such as Yahoo does not suffice for contract liability."[90]

Thus, it seems that courts will not hold a dating website liable for a contractual breach of their general assertions that they will moderate their website. The ruling in *Barnes*, however, may have left the door open for dating websites to be held contractually liability for more explicit promises.[91]

A second threshold contract question revolves around so-called "clickwrap agreements"—contracts of adhesion that purport to absolve the OSP from every imaginable form of liability.[92] Internet contract jurisprudence suggests that clickwrap agreements are generally enforceable against users.[93] A user's failure to read the online terms is not a legitimate defense to the enforceability of a clickwrap agreement's terms and conditions.[94] Again, this Note does not purport to delve into the intricacies of clickwrap jurisprudence or counterarguments such as unconscionability. Courts generally do not entertain the merits of such arguments, however, courts use CDA 230 to block contract-based liability theories when user conduct is at issue.[95]

Agency Liability

Under an agency theory of liability, a plaintiff would argue that a dating website should be liable for the actions of the tortfeasor-dater rather than for the website's own bad actions.[96] Unlike tort liability—which requires the dating website to have actively done something negligent or wrong—or contract liability—which requires the dating website to have broken a promise of some kind—an agency theory allows the plaintiff to directly recover for the tortfeasor-dater's bad actions. A plaintiff, to prove an agency relationship that would give rise to liability, would have to identify the dating website as the principal and the tortfeaser-dater as the relevant agent.[97]

A plaintiff could theoretically prove that such a relationship exists, under certain circumstances. To be considered a principal, the dating website would have to manifest its intent that the tortfeasor-dater act on the dating website's behalf—a factor arguably present if the tortfeasor-dater agrees to go on a date set up by the dating website.[98] The tortfeasor-dater as agent would then have to manifest its intent to be con-

trolled by the dating website—a much more difficult standard to satisfy.[99] One can envision, however, a scenario in which a dating website exerts so much control over the date-facilitation process that courts may find the control element present in the website-dater relationship.

In *Fonovisa, Inc. v. Cherry Auction, Inc.*, the court held that swap-meet owners could be vicariously liable for the infringing actions of their customers if (1) the owners had the right and ability to control the infringing activity and (2) the owners had some direct financial interest in their users' sales.[100] Although *Fonavisa* was decided in the intellectual-property context, it is a good example of a court using agency principles to hold the "host" liable for "user" action.

As noted earlier, dating websites certainly derive direct financial benefit from satisfying users' dating desires.[101] And it is reasonable to foresee that dating violence is a consequence arising out of dates with strangers.[102] Many dating websites typically operate in a "hands-off" fashion as a large database that allows users to search for each other.[103] Many dating websites also take pride in their formulae and strategies for connecting would-be-daters, however, which suggests a degree of facilitation that may trigger the control requirement for an agency relationship.[104] Under this newly-formed agency relationship, the dating website could then be liable either *Fonovisa*-style or directly for improperly selecting an agent as the tortfeasor-dater.[105]

The court in *Stratton* used the agency line of reasoning to some extent to prove the necessary link between website and moderator.[106] The argument in the dating website context would require a much further step to create a link between website and end-users. Post-*Stratton* courts generally hold that CDA 230 blocks all state civil law claims.[107] Thus, there is no reason why courts today would allow recovery on an agency theory. However, courts might consider agency principles—most notably the level of control exerted by the dating website—when deciding whether to impute liability to dating websites under the guise of other plaintiff theories.

Tort Liability

A tort theory of liability would seek to punish dating websites for their own conduct or lack thereof. The most likely source of liability for dating violence would probably be under a negligence theory. Justice Learned Hand formulated his classic negligence liability theory in *Carroll Towing*: if the plaintiff's expected loss is greater than the defendant's cost of preventing that loss, then, assuming the defendant owes the plaintiff a legal duty of care, the defendant has breached his duty of care to the plaintiff.[108] The *Carroll Towing* negligence formula essentially quantifies the concept that the party with the best ability, and therefore the lowest cost, to guard against harm should bear liability for failure to prevent that harm.

A plaintiff could also try and hold the website liable for its own active fraudulent misrepresentation.[109] A plaintiff would probably bring a fraudulent misrepresentation tort claim by alleging that the dating website fraudulently induced him to join or participate by making misleading reputational promises and assertions.[110]

Courts today use CDA 230 as an absolute stone wall against tort liability for OSPs. Courts are particularly worried about the chilling effect that tort liability might have on free speech, especially in the online message-board context.[111] Courts apply similar reasoning in the dating website context to immunize dating websites against liability for their passive failure to implement safety measures—even when the would-be-dater can show that the dating website failed to conform to a reasonable standard of care.[112] As already noted, CDA 230 operates to bar all state law tort claims, and would therefore preclude negligence or misrepresentation claims when user conduct is at issue.[113]

Analysis

The Question

This Note posits that CDA 230's protection of online reputational assertions breeds a number of fraudulent interactions by dating website owners and users. Much of the current criticism of CDA 230 focuses on its inability to hold dating websites liable for its users' crimes—scamming, sexual violence, and sexual exploitation of minors.[114] Their proposed solution is simple: repeal CDA 230 protection when people on dating websites are harmed.[115]

Online dating violence is a real problem,[116] as is fraud among dating website users.[117] The moral plea is compelling: why should dating websites get a pass simply because they are hosted on the Internet? Let us consider a real-life anecdote. On the television program, "The Dating Show," a lucky bachelorette selects her date from among three individuals after asking questions. [118] The show selected Rodney Alcala as a contestant, despite Rodney's two criminal convictions—one for the rape and beating of an eight-year-old girl.[119] Years later, the police discovered that Rodney was in fact a serial killer who committed many of his murders during the few years before and after his appearance on the show.[120] The lovely bachelorette selected Rodney as her date on this particular Dating Show episode.[121] Somehow, fortune intervened and the two did not actually go on a date.[122]

But what if they had? What if Rodney had killed the woman? In that case, surely we would hold "The Dating Show" civilly liable for negligently failing to sufficiently check Rodney's background before introducing him as a contestant on a dating show.[123] Why should the Internet be held to a different standard than a real-life equivalent?

This Note argues instead that dating websites are actively at fault for affirmatively defrauding their users through dishonest reputational assertions, and are able to hide behind CDA 230's all-encompassing shield. This Note proposes that much of the current fraud, committed by both dating websites and website users, would be best dealt with through imposing contract liability, even under issues that courts currently hold CDA 230 to bar.

The current criticism is focused on the wrong things. Many CDA 230 reformers have suggested bad solutions to the wrong problems as a result of their misplaced focus on dating websites' passive failure to stop harm. One author suggests that all dating websites should be required to verify the age and identity of online daters through social security number checks.[124] Another suggests requiring dating websites to check every user against an online database of registered sex offenders.[125]

There are obvious privacy implications for both of these solutions. Requiring dating websites to run database checks on potential daters would impose arguably impose only a small and justifiable burden. However, administrative oversight would be required to confirm that the database checks were actually being run. Furthermore, the Internet is global, and thus such a requirement would likely just send many websites oversees beyond the reach of American jurisprudence.

Social-security-number verification checks seem like a security nightmare. First, many internet dating websites are foreign-headquartered, such as Canada's PlentyOfFish,[126] Russia's Mamba,[127] or France's Meetic,[128] all boasting user-bases comparable to the largest U.S. dating websites. Even if dating websites are not completely-foreign entities, many of their components, such as hosting and tech support, may very well be outsourced to other countries.[129] It seems to be enough of a headache for the U.S. government to check every U.S. website offering government-mandated social-security-number verification. This will be even more of a problem, both from a jurisdictional standpoint and from a security standpoint, if much of that verification takes place oversees. Imagine calling an overseas tech support line and a scheming individual, outside of U.S. governmental reach, requests your social security number for "verification" so he can fix whatever technical problem is ailing you.

Second, because individuals will reasonably expect legitimate social security checks when signing up for certain things online, they will likely be less skeptical of illegitimate phishing schemes, where malicious individuals link to fake websites that look like legitimate websites and steal users sensitive information.[130] Imagine a "spoofed" e-mail[131] from what appears to be Match.com, asking you to update your profile with social security number verification. Under the current paradigm, most users would be incredibly wary of any e-mail that requests their social security numbers because they are not accustomed to giving their social security numbers out. If social security checks become commonplace under a legislative mandate, however, then users will have less reason to distrust e-mails asking for social security numbers.

These solutions are problematic mostly because they are entirely contrary to why CDA 230 was enacted in the first place. Their entire analysis assumes the very *Stratton*-esque premise that "the [dating] website is in the best position to protect subscribers against the false materials because it is the only party that can verify whether the information is true."[132] This is core negligence analysis: the dating website has the lowest burden to prevent the harm, thus we impose liability. But this argument goes against the very text and purpose of CDA 230: to protect the free-flow of information over the Internet by disallowing courts from treating OSPs "as the publisher or speaker" of user information.[133] This Note argues that CDA 230 has been systematically misapplied by courts to cover the wrong kind of harm, not that CDA 230's entire premise is flawed.

CDA 230 critics are reaching bad solutions because they are looking to the wrong problems. To blame dating websites for being conduits to dating violence gives dating websites far too much credit. It relegates them to mere passivity for their failure to stop harm within their grasp. This analysis is self-defeating. A completely passive dating website would operate merely as a forum for interaction, much like a sidewalk corner or campus bulletin board. We want our internet to be a bastion for interaction where users can freely post information. The problem with dating sites arises when they begin to acquire particular subsets of potential Internet daters through misrepresentations and false promises. The purpose of CDA 230 reform should not be to protect daters from other daters—although this may occur as an incidental benefit. CDA 230 should be reformed so that the government can protect daters from dating websites.

But what about the children? What of the battered victims? What about fraud? Potential victims would be better off without dating websites having negligence liability. Negligence

liability would just force dating websites out of the market, or subject potential daters to heavily-controlled and extensive contractual meandering. Or worse, entirely foreign-based dating websites, completely beyond the United States' ability to exercise any sort of control, would control the market. Given that our hypothetical victims signed up for the dating website in the first place, it is a fair assumption that our hypothetical victims would prefer a world with dating websites than a world without.

Victims would instead benefit more from contract liability. If CDA 230 protection is peeled back to allow dating websites to freely contract, then the users will be able to select the dating website that offers them the level of protection that they desire.[134]

Two cases are illustrative of the fraudulent atmosphere on the part of dating websites. First, we have the dubious promises of extramarital debauchery with AshleyMadison. Second, we have the "flirts-for-hire" of Mate1.

AshleyMadison

AshleyMadison is a dating website that caters specifically to married individuals.[135] AshleyMadison's premise is controversial on its face: "Affairs Guaranteed!"[136] This seems to be a blanket assertion that a user, after signing up for AshleyMadison's services, will successfully have an extra-marital affair. AshleyMadison makes a number of other reputational assertions on its website. It promises that other individuals are looking for the same thing, that all users are over 18, and that it is the most successful website for "finding cheating partners."[137]

AshleyMadison may be morally objectionable,[138] but immorality alone does not justify legal action.[139] AshleyMadison's conduct is objectionable because of its business model. AshleyMadison targets a class of individuals who are least likely to pursue legal action for an unsatisfactory experience: unfaithful spouses. It seems that affair-seeking is not nearly the guaranteed success that AshleyMadison may have you think—far from it.[140] And AshleyMadison runs up massive charges for lonely men looking for the few females that do exist on the website.[141] AshleyMadison has a standard clickwrap agreement disclaiming all imaginable liability.[142] But such an agreement is largely unnecessary. CDA 230 would likely preclude the plaintiff from even making an inquiry into the validity of such a disclaimer.

The success or failure of an AshleyMadison user's sexual affair is entirely dependent on the other AshleyMadison users. After all, users would have no complaint against AshleyMadison if every user agreed to a sexual hookup upon any request. To put it another way, holding AshleyMadison liable for fraudulent misrepresentation or breach-of-contract would require treating it as responsible for its users' content—namely for female user responses, or lack thereof, to male users. Thus, AshleyMadison's reputational claims—that affairs are guaranteed, that all users are looking for cheating partners, and the website is the most successful around—are all completely shielded by CDA 230.[143] This argument is a bit different than the plaintiff's claim in *Zeran*—where the court barred a libel claim under CDA 230 because it would directly implicate the web forum as responsible for users' libelous statements.[144] Courts, however, still apply CDA 230 to block contract and tort claims that indirectly implicate OSPs as responsible for user speech and conduct.[145]

Mate1

Mate1 is, at face value, a fairly standard dating website.[146] But Mate1 has a secret weapon in its cupid arsenal—the hired gun. Mate1 actively pays women to chat with male members.[147] Mate1's flirts-for-hire (Online Ambassadors) have profiles and are free to select who they communicate with.[148] Mate1 has explicitly received complaints from former users that these Mate1 "ambassadors" have contacted them under the auspices of genuine flirtatious interaction, but instead use pre-scripted lines to convince users that women are seeking them on the dating website.[149]

Why is this wrong? After all, the men are paying for and receiving female interaction. And more importantly, had the Mate1 ambassador never been hired, the user would simply had received one less interaction. It is difficult to see how the Mate1 user was specifically harmed beyond feeling a bit silly after learning that the pretty girl calling him "honey" was actually a paid Ambassador.[150] However, given the complaints received, Mate1 customers certainly appear to feel slighted in some way.[151] After all, the user's end goal was finding a date—an end goal that will likely not occur with a paid Mate1 representative. Users waste time communicating with Ambassadors, and continue to waste time and money on an ineffective website due to the false hope engendered by Mate1 flirts-for-hire. This is a reputational issue. Mate1 is artificially inflating their reputation by boosting the number of female profiles and increasing response rates through hiring paid representatives.[152] Mate1 is therefore defrauding users from the dating service that they reasonably expected when they signed up. If Mate1 is not an effective dating service, it shouldn't be in the marketplace.

Mate1 acknowledges that it pays "Online Ambassadors", buried several pages deep within its lengthy User Agree-

ment,[153] and attempts to contractually push the responsibility onto their users to discern which dating interactions are real and which are scripted.[154] *Caveat emptor*: let the buyer (or dater) beware. Mate 1 also requires Ambassadors to have a small "OA" mark in their profile defining their status.[155] However, Mate1 expressly states that it will not verify the Ambassador's profiles, tags, or communications, thus Mate1 has no control over whether Ambassadors actually actively inform users of their status.[156] And there is no reason to believe that a new Mate1 user would have any idea what the symbol "OA" means, unless they perused the extensive and small-font User Agreement. Ambassadors seemingly have no incentive to correct a user's perception of them as a friendly flirt. After all, the Ambassador's paycheck depends on Mate1, who would prefer users to feel as though Mate1 is a successful dating website. Thus, it comes as no surprise that users continue to file complaints after learning that their potential better-halves were merely Mate1 flirts-for-hire.[157]

Under the previously outlined contract-liability protection implicit in CDA 230, it doesn't seem likely that a court would hold Mate1 liable for misrepresentation or breach-of-contract. A plaintiff would have to prove two separate legal theories, given the current interpretation of CDA 230, to hold Mate1 liable under a contract theory. First, the plaintiff would have to show that the Ambassador caused a contractual violation of some sort—that the plaintiff expected and paid for some degree of service that he reasonably expected yet didn't receive.[158] As a part of this argument, the plaintiff would also have to defeat any disclaimer Mate1 made in its clickwrap User Agreement.[159] Second, the plaintiff would have to show an agency link from Mate1 to its ambassadors.[160] The plaintiff may be able to circumvent CDA 230 on the agency link. It doesn't seem as though Mate1 hiring Ambassadors in and of itself implicates user conduct in any way, and courts have found agency links between websites and non-employee helpers after CDA 230 was enacted.[161] However, the plaintiff will probably face a much tougher battle getting a court to even listen to arguments regarding the first link in the liability chain.

Mate1 users would likely not fare any better under tort law. Fraudulent misrepresentation is a state-law tort,[162] and thus will be barred by CDA 230 if the fraudulent misrepresentation was dependent on user conduct in any way.[163] The court in *SexSearch* barred the plaintiff's fraudulent misrepresentation claim because SexSearch.com's terms of service did not promise age-verification and indeed clearly disclaimed all responsibility for verifying user ages.[164] Here, a plaintiff's fraudulent misrepresentation case would be similarly based on information arguably contained within the terms of service—the existence of Mate1 Ambassadors.

Further, the user's dating website experience and success are, as with AshleyMadison, entirely dependent on other users' conduct. The central focus of the plaintiff's claim would be that Mate1 lulled them to pay for an ineffective dating service, not that the Mate1 Ambassador somehow harmed them physically or emotionally through their pre-scripted conversation. Mate1 users are harmed because Mate1 artificially inflated its female presence.[165] However, to hold Mate1 liable for fraudulent misrepresentation, the court would have to treat Mate1 as responsible for the small number of women on the website, and for those women's lack of interest toward the plaintiff. This claim would therefore not survive under CDA 230.[166]

Men are not the only ones upset with Mate1. Women have also complained about Mate1's bait-and-switch on their privacy policy—Mate1 granted men access to female users' personal contact information rather than merely their Mate1 contact information.[167] The potential for fraud, abuse, and violence is staggering here. This seems to be a standard contract issue—women gave up private information expecting a certain level of privacy protection and were later denied that same protection when Mate1 decided it would derive a greater benefit.

Liability Under Barnes and Roommates

Exploited users, female and male, may retain a glimmer of hope under *Barnes* that they may recover damages under a contract theory.[168] But dating websites are (usually) not foolish enough to include promises such as "AshleyMadison is fully responsible for ensuring, without a shadow of a doubt, that you will have extramarital relations within the next week" in their terms of service. Courts can much more easily turn a blind eye when the dating website can make a rational argument that user conduct is at issue.[169]

The key to unlocking CDA 230's stone wall against liability may lie instead with the provider-host dichotomy of *Roommates* and *Craigslist*.[170] But a dating website need only show that they didn't directly provide some form of check-box content, and the court will likely turn a blind eye.[171] Mate1 and AshleyMadison simply do not have the kind of content control required by *Roommates* to qualify them as content-providers. More likely, a court would consider these dating websites as merely providing users a "place for people to post" their dating profiles.[172]

But are we really okay with this classification? There seems to be something philosophically wrong with allowing

a website—which is already uniquely positioned within the marketplace to take advantage of clients—to lie about its reputation in order to acquire users, and then face no legal liability for that lie.

CDA 230 Judicial Interpretation: What Happened?

In *Jane Doe v. MySpace*, the trial court seemed worried about requiring OSPs to implement excessive "gatekeeping" measures to prevent every possible instance of user fraud and abuse.[173] Requiring such measures could have a severe "chilling" effect on OSPs' ability to allow their users the freedom to publish material on their websites. This chilling effect would both destroy user freedom and possibly stymie any provision of online services. Courts may have twisted CDA 230, excessively protecting OSPs in an effort to prevent this future chilling effect.

Undoubtedly, the court in *SexSearch* was also concerned about potential chilling effects on online social networking.[174] Much of the court's decision, however, was driven by the fact that the plaintiff was a statutory rapist.[175] Put simply: the court was likely uncomfortable with allowing a criminal to hold a service liable for failing to properly identify his victim's age.[176] The court may have been nervous about creating any case-law that would mitigate an individual's burden to verify that his potential sexual partner is over the age of consent. Regardless of the *SexSearch* court's ultimate motivation, the resulting case law created a dangerous liability regime.

Free Market

CDA 230 purports to have the purpose of "preserving . . . the free market" of the Internet.[177] Courts' current interpretation of CDA 230, however, is detrimental to the free market for several reasons.

First, courts' current interpretation of CDA 230 actively undermines the individual right of contract. If courts refuse to remedy breaches of affirmative promises, there is no "bite" behind the dating websites' promises. Even if both customer and dating website wanted to make an enforceable contract to, say, guarantee that no users are felons, courts would not enforce the contract under CDA 230.[178] Essentially, CDA 230 denies both dating websites and their patrons the ability to *meaningfully* enter into a *binding* agreement—despite a desire by *both* parties to contract.

Well-meaning dating websites are harmed because the law does not support and enforce their reputational promises. A dating website may make all kinds of promises and assertions, but cannot use the force of government to assuage users' mistrust of their veracity. The dating website has no more authority behind its statements than does a sleazy politician making never-to-be-followed campaign promises. In essence, a dating website loses the ability to meaningfully contract, with regard to its own reputation, with paying customers.

Well-meaning consumers will therefore also be harmed because they cannot trust promises made by dating websites. After all, if dating websites can break promises without fear of legal retribution, then most rational consumers have ample reason to shy away from relying on those promises. If consumers cannot rely on dating websites' promises, then they will be unable to find the "best" dating website for them. For example, if Joey Lonely is interested in pursuing a wide-range dating approach by talking to as many women as quickly as possible before delving further into a relationship, then he would be drawn to a website that boasts about quick response times and a large user base. However, all websites have the same incentive to cater to users such as Joey, even if they may have more or less effective business strategies and higher or lower market capitalization. Match.com may be exactly what Joey is looking for, but if the hypothetically far inferior Candle.com can make similar claims, then Joey may spend his time and money on Candle.com instead of Match.com. In fact, this scenario is more likely to occur because dating websites that offer less will likely be able to charge less.

Without accountability for reputational assertions, non-identical dating websites can make identical reputational claims even though some websites will ultimately be more effective than others. Ineffective dating websites can flourish just as well as effective dating websites. In a sense, eDarwinism cannot function properly to weed out inefficiencies in the proverbial genetic pool of the internet, and the market will suffer as a result. Dishonest dating websites can actually benefit through luring customers in under false pretenses.

Dishonest customers also benefit through lesser judicial scrutiny of their dishonest actions, combined with the false-promises of user verification. Suzy Scammer and Bradley Tortfeasor have two things going for them if they want to take advantage of dating website users. First, Suzy and Bradley can create fake profiles and not have to worry about the dating website being judicially compelled to actually verify their information, even if the dating website expressly promised to verify all profiles.[179] This means that Suzy and Bradley can target victims without risking their personal identities being discovered once the victim tries to track them down. Furthermore, victims may be lulled a false sense of security that the dating website is purportedly checking all profiles.

Thus, this interpretation of CDA 230 actively encourages lying by both dating websites and end users. This may further the stereotype that "the Internet is different," and breed a general culture that "the Internet cannot be trusted."[180] From an immediate and practical perspective, Joey Lonely may be deterred from entering into the dating market at all because of the possibility that his money and time will be wasted, or worse, that he will suffer additional fraud on the part of dishonest websites or users. Think of this as a "lemon effect," as if Joey were car shopping on Craigslist without running a title search or accident report. Most of us would consider this downright foolish, yet this is exactly the effect that CDA 230 has on the market. To put it in economic terms: consumers and producers lose out on potential mutually-beneficial trades because of an artificial fear of dishonest behavior.

From a philosophical and long-term perspective, the view that "the Internet is different" may cause addition problems. First, it can cause judges to make misguided decisions, simply because technology is involved, which could lead to dangerous precedent.[181] Second, it can stunt growth in, and adaptation to, the benefits of a globalized Internet by frightening away tentative users.[182]

This fear, however, may not be completely unfounded. After all, in some regard the Internet really is different: Internet users can far more easily hide their identity and falsify information.[183] Supporters of the current CDA 230 standard can certainly make the "strangers with candy" argument that the burden should fall on Internet users to have a healthy fear and mistrust of online dating sites.

However, fear and mistrust should be rational responses to actual problems, not generic responses to the vast uncertain territory of dating websites or the Internet. The more trustworthy information the user has, the more focused her fear and mistrust can be. And contract liability, along with liability for fraudulent misrepresentation, will best promote access to trustworthy information. This will protect the user from entering into a narrow subset of bad situations with unwanted results, without preventing the user from entering into the broader set of situations with beneficial results. The government's role should be "promote the continued development of the Internet,"[184] not stymie it.

Unintended Consequences

If potential attackers know that dating websites are not liable for failure to keep their promises regarding user safety checks, they will be more willing to create accounts on these websites.[185] Furthermore, once the potential attacker gains access to a dating website, he will be more willing to submit fraudulent information—knowing that the website will not actually verify it. A victim of violence as a result of an Internet date may, thus, be unable to track down her attacker.

Thus, by refusing to hold dating websites liable for their broken promises, courts are effectively denying victimized users two possible remedies. First, by essentially encouraging deceit in dating website profile information, courts make it more difficult for victims to track down their actual attacker. Second, by shielding the website that facilitated the harmful date from liability, courts are denying victimized users their only other remedy for the harm inflicted upon them. Thus, victimized users are left without *any* remedy whatsoever for Internet dating violence.

Proposal

Judicial Change

Courts swung way too far in their application and interpretation of CDA 230 by allowing dating websites to get away with making unenforceable promises. CDA 230 was not intended to "prevent the enforcement of all laws online."[186] Rather, it was intended to "encourage interactive computer services . . . to police . . . content without fear that through their 'good [S]amaritan . . . screening of offensive material,' they would become liable for every single message posted by third parties on their website."[187] Instead, courts created a liability structure that benefits neither website, nor user; destroyed individuals' ability to freely contract; and promoted a system of arbitrage that subsidizes Internet dating violence. CDA 230 should not bar liability for contractual breaches, such as when a dating website makes affirmative promises or assertions of factual characteristics.

Agency and Negligence Liability Are Not Answers

CDA 230 should bar some level of tort liability, such as basic negligence, which doesn't implicate the dating website's active bad actions. As the court reasoned in *Zeran*, tort liability could chill websites from providing a platform for users' free speech and conduct.[188] This chilling effect is a legitimate concern when a dating website has little or no control, beyond completely barring user speech, over its potential exposure to liability. Thus, if a dating website passively fails to verify user characteristics, absent a contractual promise to do so, it should not be liable.

CDA 230 should also operate to bar vicarious liability in the agency context. The hallmark of vicarious liability is the principal's ability to control the agent.[189] It would be a stretch to suggest that dating websites actively control their users.

Nor would we *want* users to be able to assert such a relationship. The same speech-chilling concern with negligence liability applies here with even greater force. At least in the negligence context, the dating website would have to fail to meet some basic standard of care, however nebulous that standard may be.[190] In the agency context, a dating website could be held liable completely independently of any of its own bad actions.[191]

When the dating website crosses the line into gross negligence or fraudulent misrepresentation, however, its conduct seems (1) actively wrongful and (2) entirely within its control. Furthermore, dating websites are uniquely positioned to prevent certain identifiably dangerous people, such as felons, from using their website as a platform to find victims.[192] It doesn't seem unreasonable as a policy matter to incentivize dating website to take steps, such as credit card verification or running criminal background checks, to screen such individuals without disrupting their users' free speech.

Dating websites will, to some extent, self-regulate if they are able to freely contract. Basic economic theory postulates that consumers will, if given full information, consistently pick the option best suited to their needs. And free contracting allows consumers the ability to trust the information provided by dating websites in the form of enforceable reputational assertions and promises.[193] Thus, if a large enough subset of potential daters would prefer a certain set of privacy preferences, then the dating websites that provide that set of privacy preferences will retain a user base. Conversely, those dating websites that fail to provide the set of privacy preferences will lose out on that subset of potential daters, and eventually be driven out of the market.

Legislative Change: Safe Harbor

Congress should also adopt an additional "safe harbor" provision that clearly delineates the standard of care that a website can take to avoid negligence liability for user action. To be fair, the anonymity and "arms-length" nature of the Internet makes it difficult for a website to always effectively verify its user's attributes.[194] Thus, instead of legislatively requiring websites to run certain types of background and identity checks, courts should instead clearly define the standard of care that a website may meet to avoid tort liability. This Note suggests two "safe harbor" provisions to protect dating websites[195] from unfair liability under CDA 230. First, if a website runs a criminal background check on a user and it returns negative, then the website should be allowed an affirmative defense that presumptively imputes to the website reasonable knowledge that the user was not a felon. Second, if the website requires that users sign up with a credit card, the website should be allowed an affirmative defense that presumptively imputes to the website reasonable knowledge that the user was over eighteen years old.

Each individual can more freely take on the risk of online dating if that risk is circumscribed by tort liability outside of the "safe harbor." Dating websites can also operate more freely if they can reference a clearly delineated standard of care. At the same time, a dating website that operates outside of the safe harbor—and is therefore potentially liable for tort damages—is arguably culpable because it actively failed to take precautions that it knew were clearly enumerated.

This safe harbor can also operate to protect dating websites from certain kinds of inadvertent contractual liability. If a dating website uses the properly outlined safe harbor verification methods on all users, it can in good faith make the assertion that "all users are over 18" or that the website contains "no felons," and suffer no contractual liability if one user somehow manages to fool the verifications.

Conclusion

Much of the current analysis of CDA 230 liability is wrongly focused on negligence liability and the very specific group of violent offenders who use dating websites to find victims. CDA 230 has, however, spawned far broader problems by creating counterintuitive liability immunity that mostly benefit fraudulent service providers and users. The legislature and courts need to re-evaluate CDA 230 within its intended framework: to "promote the continued development of the Internet."[196]

Holding dating websites liable for their affirmative promises and assertions will, at worst, compel those websites to refrain from making promises they cannot keep. It will protect the dating websites' autonomy to make rational choices about the sorts of *enforceable* contracts they wish to make with users. It will protect users' access to trustworthy information, and therefore protect users' autonomy to make rational and *informed* choices. It will create the safest online dating environment without chilling users' ability to freely flirt and find a match. And it may prevent Rodney Alcala from becoming your next online date. ▪

Endnotes

1 Andrew S. Trees, Decoding Love 14 (2009).

2 Scott Adams, Dilbert, Oct. 14, 1994, *available at* http://dilbert.com/strips/comic/1994-10-14/.

3 *See* Javier Espinoza, *Online Dating Sites Flirt With Record Growth*, Forbes (Jan. 6, 2009), http://www.forbes.com/2009/01/06/online-dating-industry-face-markets-cx_je_0105autofacescan01.html ("With the current downturn in the economy, soul seekers are turning away from traditional and expensive methods of meeting people casually in bars and instead are flocking en masse to online dating services, with some of the sites posting 400.0% sales growth year on year.").

4 47 U.S.C. § 230 (1996).

5 47 U.S.C. § 230(c)(1).

6 *Infra* part IV.

7 *Infra* part IV.C.

8 *Infra* part IV.A.

9 *Infra* part II.B.

10 *Infra* part IV.

11 *Infra* part VI.

12 AshleyMadison, http://AshleyMadison.com; *id.* ("100% Discreet Like-minded people").

13 *Infra* part VI.A.

14 *Infra* part VI.B.

15 Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. 1995). In *Stratton*, the defendant Prodigy hosted an online message-board called "Money Talk," on which users may post content moderated by Prodigy's Board Leaders. *Id.* at 3. An unidentified individual posted statements about Stratton suggesting *they* were involved in criminal activity, for which Stratton sued Prodigy as a content provider for libel. *Id.* at 2. The court held first that Prodigy was a publisher of the libelous information and therefore liable for the content. *Id.* at 10–11. The court then held that Prodigy was liable through an agency theory for the Board Leader's failure to remove the libelous post. *Id.* at 17–18.

16 *Id.* at 10–11.

17 47 U.S.C. § 230 (1996).

18 *See* 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

19 *Id.*

20 Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998). In *Zeran*, an anonymous individual prank-posted on AOL's online message-board an advertisement for sale of offensive t-shirts related to the Oklahoma City bombing, and included Kenneth Zeran's phone number as a contact. *Id*. at 329. As a result, Mr. Zeran received a number of phone calls—some of which were death threats. *Id*. Mr. Zeran contacted America Online to remove the post, but AOL did not take immediate action. *Id*. After the postings continued, Mr. Zeran sued AOL for negligence, claiming that AOL unreasonably delayed removing the posts. *Id*. The court upheld the district court's dismissal of the case due to CDA 230 immunity. *Id.* at 335.

21 *See id.* at 334 ("Congress' desire to promote unfettered speech on the Internet must supersede conflicting common law causes of action.").

22 *Id.* at 329.

23 *Id.*

24 *Id.* at 332–33.

25 Doe v. SexSearch, 502 F. Supp. 2d 719 (N.D. Oh. 2007), *aff'd* on non-CDA 230 grounds by, *Doe v. SexSearch.com*, 551 F.3d 412 (6th Cir. 2008). In *SexSearch*, an adult male, the plaintiff, met an underage girl, Jane Doe, on SexSearch.com—an adult website that facilitates sexual encounters. *Id.* at 722. The plaintiff was arrested for unlawful sexual conduct with a minor and sued SexSearch.com for, among other things, breaking its warranty that all users are over 18 years of age and failing to remove Jane Doe's profile. *Id.* at 722–23. The court held that CDA 230 blocked all of the plaintiff's claims—except for a separate unconscionability claim that the court denied on other grounds—because holding SexSearch.com liable would require treating it as the publisher of the girl's profile. *Id.* at 727–28.

26 *Id.* at 722.

27 *Id.* at 723.

28 *Id.* at 722.

29 *Id.*

30 *Id.* at 723–24.

31 *Id.* at 727–28.

32 Jane Doe v. MySpace Inc., 528 F.3d 413 (5th Cir. 2008). In *MySpace*, a nineteen-year-old male met the plaintiff, thirteen-year-old Jane Doe, on social networking website MySpace.com. *Id.* at 416. Doe lied about her age in order to join MySpace.com and circumvent safety features, which violated MySpace.com's terms of service. *Id.* The two arranged a physical meeting, whereupon the man sexually assaulted Doe. *Id.* Doe sued MySpace.com for failing to implement proper safety precautions to ensure that minors could not create a profile and circumvent MySpace.com's existing safety precautions. *Id.* at 417. The court held that CDA 230 barred Doe's claims, because holding MySpace.com liable would require the court to treat MySpace.com as the publisher of Jane Doe's profile. *Id.* at 422.

33 *Id.* at 415.

34 *Id.*

35 *Id.* at 416.

36 *Id.*

37 *Id.*

38 *Id.* at 416, 421.

39 *Id.* at 422.

40 *See generally Finding true love: A look at the history of dating*, MSNBC Today (Feb. 17, 2005, 10:40 AM), http://today.msnbc.msn.com/id/6967668/ns/today/t/finding-true-love-look-history-dating/#.Tqx9_t77j2s.

41 *Id.*

42 *Id.*

43 *Id.*

44 *Your Big Moment*, IMDB, http://www.imdb.com/title/tt0041009/.

45 *Finding true love: A look at the history of dating*, MSNBC Today (Feb. 17, 2005, 10:40 AM), http://today.msnbc.msn.com/id/6967668/ns/today/t/finding-true-love-look-history-dating/#.Tqx9_t77j2s.

46 *See, e.g.*, *Relationships in The Facebook Era [Advice From Men]*, Dating Without Drama, http://www.datingwithout-drama.com/relationships-in-the-facebook-era-advice-from-men/; Julia Boorstein, *The Big Business of Online Dating*, CNBC Media Money (Feb. 12, 2010), http://www.cnbc.com/id/35370922/The_Big_Business_of_Online_Dating ("Forty one percent of online daters say they also use sites like Facebook to find dates."). The Author can also personally attest to the fact that Facebook plays an integral role in modern social interaction: both in comfortably getting to know other people and in facilitating flirtation.

47 *See* Boorstein, *supra* note 46 ("Online dating isn't just about making love connections, it's about making lots and lots of money. And as the stigma of meeting a match online falls by the wayside, the industry's growth is accelerating. Online dating revenues are growing 10 percent to 15 percent per year . . . .").

48 *Id.*

49 "Check-the-box" options offered by many dating websites allow users to select characteristics that they feel represent who they are. The options are provided by a site. But the user decides what representations to make and whether to represent a characteristic at all. An example of this is Facebook's drop-down list of "relationship status." *See Drop-Down List*, Facebook, http://www.facebook.com/pages/Drop-down-list/108451612512403. If a user decides to represent to others that he is or is not in a relationship, the user may only select from Facebook's preselected choices for relationship status (e.g. "single," "married," "it's complicated"), and may not define their own category.

50 *Id.*

51 *See, e.g.*, ChristianSingles, http://www.christiansingles.com ("dedicated to marriage minded Christian singles.").

52 *See, e.g.*, AshleyMadison, http://AshleyMadison.com ("All Members are 18 or Over"); *id.* ("100% Discreet Like-minded people").

53 *See, e.g.*, ChristianSingles ("To ensure online safety, all of our new members are approved manually."); True, http://www.True.com (promising "[c]riminal screenings for felonies").

54 *See, e.g.*, AshleyMadison ("AFFAIRS GUARENTEED").

55 *See* Doe v. SexSearch.Com, 502 F. Supp. 2d 719, 727 (N.D. Oh. 2007) (holding that the court would have to treat SexSearch.com as the publisher of Doe's profile to hold it liable for several tort and contractual violations, which would contravene CDA 230's express provisions).

56 *See* Jane Doe v. MySpace Inc., 528 F.3d 413, 418 (5th Cir. 2008) ("Courts have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content.").

57 *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) ("Under § 230(c), therefore, so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process."). In *Carafano*, an anonymous individual impersonated famous actress Christianne Carafano on a dating website by posting sexually suggestive content along with the actress' actual phone number and e-mail address. *Id.* at 1121. As a result, Ms. Carafano received a number of sexually explicit calls and messages, and felt unsafe in her home. *Id.* at 1122. Ms. Carafano's agent contacted the website to have the profile removed, which the website promptly did. *Id.* Ms. Carafano sued for "invasion of privacy, misappropriation of the right of publicity, defamation, and negligence." *Id.* The court held that CDA 230 provided immunity to the dating website on all counts, because the dating website did not create or develop the information at issue. *Id.* at 1125.

58 *See* Julie Doe II v. MySpace Inc., 175 Cal. App. 4th 561, 573–74 (2009). In *Julie Doe II*, a combination of four essentially identical cases, fifteen-year-old MySpace user Julie Doe was drugged and sexually assaulted by an individual she met on MySpace. *Id.* at 565. Doe sued MySpace for negligence in failing to implement reasonable safety precautions, including age-verification software. *Id.* The court rejected Julie Doe's argument that MySpace "collaborated with the Does" and held instead that MySpace "did nothing to encourage the posting of such content"; thus, MySpace was immunized from liability by CDA 230. *Id.* at 574–75.

59 *See id.* at 567 ("Immunity under [CDA] section 230 requires proof of three elements: (1) MySpace is an interactive computer services provider, (2) MySpace is not an information content provider 4 with respect to the disputed activity, and (3) appellants seek to hold MySpace liable for information originating with a third party user of its service.").

60 *See* Doe v. SexSearch.com, 502 F. Supp. 2d 719, 727 (N.D. Ohio 2007) ("Thus, the CDA grants immunity from all civil liability, except for the few exceptions expressly laid out in the statute: (1) federal criminal law; (2) intellectual property law; (3) State law that is consistent with this section; and (4) the Electronic Communications Privacy Act of 1986.").

61 *See id.* (holding that SexSearch.com was not liable to a man after he had a sexual encounter with a minor through SexSearch.com, even after SexSearch.com guaranteed that all members were eighteen or over).

62 *See* 47 U.S.C. § 230(e) (listing the exceptions to CDA 230 immunity).

63 47 U.S.C. § 230(c)(1).

64 *See* Julie Doe II v. MySpace Inc., 175 Cal. App. 4th 561, 575 (2009) ("MySpace was not an information content provider subject to liability under section 230").

65 *See id.*

66 Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008). In *Craigslist*, the defendant-OSP Craigslist provided a website that allowed users to post advertisements and notices in various categories—including a housing subsection. *Id.* at 668. Plaintiff sued Craigslist for violating the Fair Housing Act due to certain user housing advertisements that made discriminatory comments such as "NO MINORITIES." *Id.* at 668. The court held that Craigslist was not liable under the Fair Housing Act, because CDA 230 disallowed the court from holding Craigslist as the publisher of the discriminatory advertisements. *Id.* at 671.

67 *Id.*

68 *Id.*

69 Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008). In *Roommates*, the defendant-OSP provided a website for users to sign up and post advertisements for house rentals. *Id.* at 1161. Roommates.com permitted users to select checkboxes for roommate preferences—including "sex," "sexual orientation," and "children in household." *Id.* Plaintiff sued Roommates.com for violating California housing discrimination laws by allowing users to discriminate through selecting checkboxes in a discriminatory fashion and posting discriminatory "additional comments." *Id.* at 1162. The court held that CDA 230 did not apply to the check boxes because Roommates.com provided the content contained therein, and therefore held Roommates.com liable for discriminatory housing practices. *Id.* at 1170. The court held, however, that CDA 230 immunized Roommates.com from liability for the content that users posted in the "additional comments" section because the content was provided by the user and merely hosted by Roommates.com. *Id.* at 1174.

70 *See id.* at 1172 ("Roommate is directly involved with developing and enforcing a system that subjects subscribers to allegedly discriminatory housing practices").

71 *Infra* part IV.

72 *See* Gentry v. eBay, Inc., 99 Cal. App. 4th 816, 833 (2002) ("It is not inconsistent for eBay to be an interactive service provider and also an information content provider; the categories are not mutually exclusive. The critical issue is whether eBay acted as an information content provider with respect to the information that appellants claim is false or misleading.").

73 *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) ("Under § 230(c), therefore, so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process.")

74 47 U.S.C. 230(c)(2) ("No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be . . . objectionable . . . .").

75 *See* Restatement (Third) of Agency § 2.04 cmt. b (2006) ("[R]espondeat superior . . . establishes a principle of employer liability for the costs that work-related torts impose on third parties. Its scope is limited to the employment relationship and to conduct falling within the scope of that relationship because an employer has the right to control how work is done.").

76 *See, e.g.*, *id.* ("Respondeat superior is inapplicable when a principal does not have the right to control the actions of the agent.")

77 *See* Raymond T. Nimmer, Law of Computer Technology § 13:27 (2011) ("Under this broad approach and the equally broad concepts of agreement followed in Article 2 and in common law, actions taken electronically clearly can provide a sufficient basis to form a contract.").

78 *See* Boorstein, *supra* note 46 ("Online dating isn't just about making love connections, it's about making lots and lots of money. And as the stigma of meeting a match online falls by the wayside, the industry's growth is accelerating. Online dating revenues are growing 10 percent to 15 percent per year . . . .").

79 *See id.* ("All these [subscription-based] premium services face competition from free sites like Plentyoffish.com, which is ad supported . . . .").

80 *See, e.g.*, Ben Axley, *Snap Interactive: Facebook's Fast Growing And Most Undervalued Social Media Company*, Seeking Alpha (Feb. 1, 2012), http://seekingalpha.com/article/331542-snap-interactive-facebook-s-fast-growing-and-most-undervalued-social-media-company ("Why has online matchmaking become so successful? The advantages for the user are numerous and include: 1) Allows for targeted searches for matches along numerous physical and personal dimensions and qualities; . . . 5) Promotes a secure and safe way to screen potential matches . . . .").

81 *See, e.g.*, True, http://www.true.com/Default.htm ("With criminal background screenings in the U.S. and Single Certification, TRUE.com is the online dating service where you can enter into any kind of relationship you're looking for – love, romance, friendship – with the knowledge that we're serious about your safety.").

82 *See, e.g.*, *Terms of Use*, True, http://www.true.com/pop-MoreText.aspx?id=6.

83 *See* Nimmer, *supra* note 77 ("Forming a contract online (or indeed in any similar setting) thus requires that, having had a chance to review the terms of the contract, a person engages in conduct that it has reason to know will indicate assent to the contract terms. As we all know, whether the person assenting to the form took the time to read it is not material as a matter of law.").

84 *See* Restatement (Second) of Contracts § 5 (1981) ("The terms of a promise or agreement are those expressed in the language of the parties or implied in fact from other conduct.").

85 *See* Doe v. SexSearch.com, 502 F. Supp. 2d 719, 727 (N.D. Ohio 2007) ("Thus, the CDA grants immunity from all civil liability, except for the few exceptions expressly laid out . . .").

86 Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009). In *Barnes*, Cecelia Barnes sued Yahoo for failing to remove compromising pictures and messages that her ex-boyfriend posted, pretending to be Barnes, on Yahoo. Id. at 1098–99. After Barnes's ex-boyfriend posted photos and messages, Barnes was repeatedly harassed by individuals expecting sexual favors. Id. at 1098. Barnes repeatedly provided Yahoo with notice of the photos and messages, but did not receive a response. Id. Finally, a Yahoo representative called Barnes and informed her that Yahoo would "take care of it." Id. at 1099. After two months of inaction, Barnes sued on two theories: (1) that Yahoo committed negligence, a state law tort, and (2) that Yahoo broke their contractual promise to remove the unauthorized posting. Id. at 1099. The court held that CDA 230 barred the state tort claim. Id. at 1102–06 However, the court held that CDA 230 did not bar a breach of contract claim under a promissory estoppel theory. Id. at 1108–09.

87 *Id.* at 1107.

88 *Id.*

89 *See id.* at 1109 ("Because we have only reviewed the af-

firmative defense that Yahoo raised in this appeal, we do not reach the question whether Barnes has a viable contract claim . . . .").

90 *Id.* at 1108.

91 *But see* Doe v. SexSearch, 502 F. Supp. 2d 719, 727–728 (N.D. Oh. 2007), *aff'd* on non-CDA 230 grounds by, *Doe v. SexSearch.com*, 551 F.3d 412 (6th Cir. 2008) (blocking Doe's contract claims under CDA 230 because contract liability would require treating SexSearch.com as the publisher of the underage girl's profile).

92 *See generally* Kevin W. Grierson, *Enforceability of "Click-wrap" or "Shrinkwrap" Agreements Common in Computer Software, Hardware, and Internet Transactions*, 106 A.L.R.5th 309 (2003).

93 *See, e.g.*, Major v. McCallister, 302 S.W.3d 227, 231 (Mo. Ct. App. 2009) ("For these reasons, Appellant's contention that the website terms were so inconspicuous that a reasonably prudent internet user could not know or learn of their existence, or assent to them without a 'click,' is unconvincing. Point denied.").

94 *See, e.g.*, *id.* at 230 ("Failure to read an enforceable online agreement, as with any binding contract, will not excuse compliance with its terms. A customer on notice of contract terms available on the internet is bound by those terms." (quoting Burcham v. Expedia, Inc., 2009 WL 586513, *2 (E.D. Mo. 2009)).

95 *See* SexSearch, 502 F. Supp. 2d at 727–728 (blocking Doe's contract claims on CDA 230 grounds without reaching the merit of his argument).

96 Restatement (Third) Of Agency § 7.03 (2006).

97 *Id.*

98 *See* Restatement (Third) of Agency § 1.01 ("Agency is the fiduciary relationship that arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act.").

99 *Id.*

100 *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996) ("[E]ven in the absence of an employer-employee relationship one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities." (quoting Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971))). In *Fonavisa*, record-company Fonavisa sued the defendant, who operated a swap meet where other users traded counterfeit Fonavisa records. *Id.* at 261. The court held that the defendant exercised sufficient control over the counterfeiters' activity by owning and operating their meeting space. *Id.* at 263. The court also held that the defendant received financial benefit from the illicit activities through sale-space reservation fees, even though they did not receive a specific "commission" from infringing sales. *Id.* The court held, thus, that the defendant met both prongs of the test for vicarious liability and was potentially liable for copyright infringement. *Id.* at 264.

101 *See* Boorstein, *supra* note 46 ("Online dating isn't just about making love connections, it's about making lots and lots of money. And as the stigma of meeting a match online falls by the wayside, the industry's growth is accelerating. Online dating revenues are growing 10 percent to 15 percent per year . . . .").

102 *See, e.g.*, Margaret Kavanagh, *Significant increase in stalkings reported with online dating* (Jan. 31, 2012), http://www.cfnews13.com/content/news/baynews9/news/article.html/content/news/articles/ot/both/2012/01/30/Significant_increase_in_stalkings_reported_with_online_dating.html ("However, as dating online becomes increasingly popular, so are problems reported to the authorities. . . . The Florida Council Against Sexual Violence said there hasn't been that much data collected on the dangers of online dating, but said there has been a significant incidents of issues being reported because dating online has become so popular.").

103 *See, e.g.*, *Quick Search*, DateHookup.com, http://www.datehookup.com/UserSummary.aspx ("Our Quick Search utility allows you to find singles fast, without getting too specific.").

104 *See, e.g.*, *What Makes Us Different*, EHarmony, http://www.eharmony.com ("When it comes to finding someone who's right for you, we think the best way we can help is by getting to know you and what you're looking for. That's why we designed our one-of-a-kind questionnaire . . . . [W]e'll introduce you to singles who truly complement you, across 29 key areas . . . . ").

105 *See* Restatement (Third) of Agency § 7.05(1) (2006) ("A principal who conducts an activity through an agent is subject to liability for harm to a third party caused by the agent's conduct if the harm was caused by the principal's negligence in selecting, training, retaining, supervising, or otherwise controlling the agent.").

106 *See* Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 N.Y. Misc. LEXIS 229, 14–18 (N.Y. Sup. Ct. 1995) (holding that Prodigy's Board Leader, who negligently failed to remove libelous material, was an agent of Prodigy for the purposes of the case).

107 *See* Doe v. SexSearch.com, 502 F. Supp. 2d 719, 727 (N.D. Ohio 2007) ("Thus, the CDA grants immunity from all civil liability, except for the few exceptions expressly laid out . . .").

108 *See* United States v. Carroll Towing Co. 159 F.2d 169, 173 (2d. Cir. 1947) ("[I]f the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B less than PL.").

109 Note that by "misrepresentation," this Note is referring to "fraud" or "fraudulent misrepresentation"—a state law tort that can apply in the consumer context. Some states, as we saw in *SexSearch*, also have the confusingly similar tort of negligent misrepresentation—which requires that improper advice be given in the context of a business relationship. *See* SexSearch, 502 F. Supp. 2d at 731 ("'[A] core requirement in a claim for negligent misrepresentation is a special relationship under which the defendant supplied information to the plaintiff for the latter's guidance in its business transaction.' . . . The transaction in the instant case is not the type of 'special relationship' required . . . for negligent misrepresentation." (quoting *Ziegler v. Findlay Indus.*, 464 F.Supp.2d 733, 738 (N.D.Ohio 2006))

110 *See* Restatement (Second) of Torts § 525 (1977) ("One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it, is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation."). This principle is also similarly presented within Contract law. *See* Restatement (Second) of Contracts § 159 (1981) ("A misrepresentation is an assertion that is not in accord with the facts.").

111 *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 ("The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings . . . interactive computer service providers might choose to severely restrict the number and type of messages posted.").

112 *See* Jane Doe v. MySpace Inc., 528 F.3d 413, 422 (5th Cir. 2008) ("[T]heir negligence and gross negligence claims are barred by the CDA [Section 230], which prohibits claims against Web-based interactive computer services based on their publication of third-party content."

113 *See* Doe v. SexSearch.com, 502 F. Supp. 2d 719, 727 (N.D. Ohio 2007) ("Thus, the CDA grants immunity from all civil liability, except for the few exceptions expressly laid out . . .").

114 *See, e.g.*, John Nisbett, Comment, *Checkmate: How Sexual Predators in (Your)Space Have Strategically Employed Existing Cyber-Laws to Outflank Their Prey,* 28 Miss. C. L. Rev. 181 (2009) ("[T]oday's sexual predators employ online social networking sites ('OSNs') as the new frontier for clandestine hunting grounds. These faceless cybersharks—the illicit spawn of the robust shelters created by § 230 of the Communications Decency Act ('CDA')—have rapidly adapted . . . .").

115 *See, e.g.*, Trenton E. Gray, Student Note, *Internet Dating Websites: A Refuge for Internet Fraud*, 12 Fla. Coastal L. Rev. 389, 390 (2011) ("Therefore, this liability should fall on the Internet dating sites, as well as the subscriber who misleads people into believing something that is not real. The dating websites should not be immune under the Communications Decency Act (CDA) as an interactive computer service . . . .").

116 *See, e.g.*, Kavanagh, *supra* note 102 and accompanying text.

117 *See BBB issues warnings about dating site scams*, The MetroWest Daily News (Feb. 13, 2012), http://www.wickedlocal.com/millis/news/x2112944180/BBB-issues-warnings-about-dating-site-scams#axzz1nFXQR8X7 ("[T]he Better Business Bureau warns there are scams as well as reputable sites, and scam artists on legitimate sites, too. Last year, 2,500 people filed complaints against online dating sites nationally, the Better Business Bureau reports. . . . '[T]he anonymity of the Internet makes it easy for con artists to use these sites to meet potential victims and prey upon lonely hearts.'" (quoting Better Business Bureau spokeswoman Paula Fleming)).

118 Mike von Fremd & Bonnie McLean, *'Dating Game Killer' Case Goes to Jury*, ABC Nightline (Feb. 24, 2010), http://abcnews.go.com/Nightline/dating-game-serial-killer-rodney-alcala-murder-trial/story?id=9924537.

119 *Id.*

120 *Id.*

121 *Id.*

122 *Id.*

123 A defendant can still be liable for negligence if he places the victim in a situation where harm by a third party is reasonably foreseeable. *See* Restatement (Third) of Torts: Phys. & Emot. Harm § 19 (2010) ("The conduct of a defendant can lack reasonable care insofar as it foreseeably combines with or permits the improper conduct of the plaintiff or a third party.").

124 *See, e.g.*, *id* at 425 ("The more reliable approach [to prevent dating-site violence] would be an identity and age verification system for Internet dating websites utilizing social security numbers.").

125 *See* Nisbett, *supra* note 114 at 202 (proposing "a legislative mandate of online registration for sex offenders").

126 *Plentyoffish Media Inc. Company Overview*, Bloomberg Businessweek, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=8345087 ("Plentyoffish Media Inc. operates as a free online dating site. It serves the users in the United States, Canada, Australia, and Europe. The company was founded in 2003 and is based in Canada.").

127 *JSC "Mamba" Company Overview*, Bloomberg Businessweek, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=25745918 ("JSC 'Mamba' operates online dating sites. It offers Internet-based acquaintance services; and Internet introductions and chat systems. JSC 'Mamba' was founded in 2004 and is based in the Russian Federation.").

128 *Meetic S.A. Company Overview*, Bloomberg Businessweek, http://investing.businessweek.com/research/stocks/snapshot/snapshot.asp?ticker=MEET:FP ("Meetic S.A. provides online dating and matchmaking services in France and internationally. . . . Meetic S.A. was founded in 2001 and is based in Boulogne-Billancourt, France.").

129 *See* Rebecca Leung, *Out Of India*, CBS News 60 Minutes (Feb. 11, 2009), http://www.cbsnews.com/2100-18560_162-590004.html (explaining that many companies now outsource call centers and other technical support features to India and other overseas countries).

130 *See generally Phishing Symptoms*, Microsoft, http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx (describing a typical phishing scheme).

131 *See generally FAQ: Spoof email*, Symantec (May. 2011), http://www.symantec.com/business/support/index?page=content&id=TECH82284 (describing spoofed e-mails as "us[ing] a false or invalid email header to describe from whom it came").

132 Gray, *supra* note 115 at 411.

133 47 U.S.C. § 230(b), (c)(1).

134 *Infra* part IV.C.

135 *See* AshleyMadison, http://AshleyMadison.com ("We are the most recognized and reputable extramarital affair company. Our married dating services work. We are the most successful website for finding cheating partners.").

136 *Id.*

137 *Id.*

138 Kashmir Hill, *Ashley Madison: Lessons In Promoting a Sleazy Business*, Forbes (Feb. 11, 2011), http://www.forbes.com/sites/kashmirhill/2011/02/11/ashley-madison-lessons-in-promoting-a-sleazy-business/.

139 Adultery is technically still illegal in many states, although this classification is constitutionally suspect. *See* Jonathan Turley, *Adultery, in many states, is still a crime*, USA Today (Apr. 2010), http://www.usatoday.com/news/opinion/forum/2010-04-26-column26_ST_N.htm ("About two dozen states still have criminal adultery provisions. While prosecutions remain rare, they do occur. And beyond the criminal realm, these provisions can be cited in divorce proceedings, custody disputes, employment cases and even to bar people from serving on juries."). The focus of this Note is not on the constitutionality of adultery laws, however.

140 *See* Sheelah Kolhatkar, *Cheating, Incorporated*, BusinessWeek (Feb. 10, 2011), http://www.businessweek.com/stories/2011-02-09/cheating-incorporated ("Just as Biderman predicted, Ashley Madison is drowning in husbands, so many that they threaten to crush the few venturesome ladies who have boldly—and perhaps recklessly—put themselves out there."); Caitlin Dickson, *How Common Is Cheating, Really?*, The Atlantic Wire (Feb. 11, 2011), http://www.theatlanticwire.com/national/2011/02/how-common-is-cheating-really/17786/ ("But are that many married people really searching for someone else? A recent study by the University of Virginia suggests the market for unfaithful spouses may be shrinking, not growing.").

141 *See id.* ("The pricing system is cleverly designed to charge the men at their most vulnerable moment . . . Creating a profile and browsing others are free, but if you'd like to initiate an e-mail or chat conversation with someone, you must purchase 'credits'—200 of them cost $79.00, and they run like a meter.").

142 *Terms & Conditions*, AshleyMadison, http://www.ashleymadison.com/app/public/tandc.p?c=1.

143 *Supra* part III.B.

144 Zeran v. Am. Online, Inc., 129 F.3d 327, 335 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998).

145 *See, e.g.*, Doe v. SexSearch.Com, 502 F. Supp. 2d 719, 727 (N.D. Oh. 2007) (holding that contract liability for SexSearch.com would require the court to treat SexSearch.com as the publisher of Doe's profile, which would contravene CDA 230's express provisions).

146 Mate1, http://www.mate1.com/nw/.

147 *See* Sarah McDaniels, *Mate1 Scam? How Free Dating Sites Lure Men*, King of How To (Feb. 13, 2012), http://kingofhowto.com/Dating/mate1-scam-free-dating-sites-526.html ("In its terms of service, this dating site freely reveals that it does in fact hire women to encourage the 'active participation' of male members on the site."); *Terms & Service*, Mate1, http://www.mate1.com/nw/ ("Company may . . . hire certain Members that have posted Profiles, who shall be called 'Online Ambassadors,' to greet and otherwise communicate with all classes of Members . . . at their sole discretion, with a view to welcoming Members and encouraging their active participation on the Site.").

148 *Id.*

149 *See, e.g.*, Skip Niemierzycki, *Complaint Review: Mate1 dating*, Ripoff Report (Mar. 29, 2010), http://www.ripoffreport.com/computer-fraud/mate1-dating/mate1-dating-i-corresponded-w-f3654.htm ("Corresponded with [Mate1] 'Ambassador' female who I thought was legitimate. After 3 weeks or so, received copy of same correspondence . . . . [O]n one of the later chats she referred to me as 'sweetie.' . . . [T]he displayed photo(s) as well as the correspondence are false!").

150 *Id.*

151 *See, e.g.*, *id.* ("I have lost complete faith in the computer dating business, and anyone who thinks they are getting a real person, behind some real honest, truthful writing, is in for a very rude awakening! The computer dating service is teaming with ripoff scoundrels; you really have no idea how many! Mate1 should be the first to be put out of business post haste.").

152 *See* McDaniels, *supra* note 147 and accompanying text.

153 *See* Niemierzycki, *supra* note 149. ("Company may, from time to time, hire certain Members that have posted Profiles, who shall be called "Online Ambassadors," to greet and otherwise communicate with all classes of Members via the Interactive Services and to help safeguard against abuse of the Agreement by reporting wrongdoing to Site administrators.").

154 *See id.* ("You are solely responsible for Your interactions with Online Ambassadors.").

155 *See id.* ("The Online Ambassadors will have the OA logo, or an Online Ambassador tag, prominently displayed on their Profiles, together with language indicating that they are sponsored by Company, and that logo will comprise an html link to an explanation of the meaning of that logo.").

156 *See id.* ("As is the case with all Members, Company is not responsible for verifying the content of the Online Ambassadors' Profiles or auditing the content of their communications via the Interactive Services, Feedback and other Content.").

157 *See* McDaniels, *supra* note 147 ("[T]here are numerous online complaints regarding a potential Mate1 scam in which some accuse the company of paying women, which it calls 'online ambassadors,' to answer emails. According to some former members, this is an attempt to bait male members along; so they'll keep renewing their membership every month.").

158 *Supra* part III.B.

159 *Supra* part III.B.

160 *Supra* part III.C.

161 *See, e.g.*, Columbia Pictures Indus., Inc. v. Fung, CV 06-5578 SVW(JCX), 2009 WL 6355911 (C.D. Cal., 2009) ("These individuals were under the control of Defendants and assigned duties related to the administration of the web forums. Therefore, there is an agency relationship between these individual moderators (or 'admins') and Defendants.").

162 *See, e.g.*, Va. Code § 59.1-200(A) (2011) ("The following fraudulent acts or practices committed by a supplier

HOME BACK NEXT

in connection with a consumer transaction are hereby declared unlawful: . . . 5. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits.").

163 *Supra* part III.B.

164 Doe v. SexSearch.Com, 502 F. Supp. 2d 719, 729–30 (N.D. Oh. 2007) ("Plaintiff cannot claim he was misled or he reasonably relied on the representation that 'all members are 18+' when the Terms and Conditions clearly state the website did not guarantee [it]. . . . Plaintiff specifically agreed to these Terms and Conditions when registering as a member.").

165 *See* McDaniels, *supra* note 147 ("The fact that Mate 1 allows women to join for free is a clear indication that the site has more male members than female ones, which is a common problem with free dating sites.").

166 *See* Julie Doe II v. MySpace Inc., 175 Cal. App. 4th 561, 567 (2009) ("Immunity under [CDA] section 230 requires proof of three elements: (1) MySpace is an interactive computer services provider, (2) MySpace is not an information content provider with respect to the disputed activity, and (3) appellants seek to hold MySpace liable for information originating with a third party user of its service.").

167 *See* McDaniels, *supra* note 147 ("Many women have complained that they've been dog-piled by sleazy messages the moment they joined the site, with some even claiming that Mate1.com somehow fails to protect their privacy, allowing men to contact them outside the platform.").

168 *Supra* part III.B.

169 *See, e.g.*, Doe v. SexSearch.Com, 502 F. Supp. 2d 719, 727 (N.D. Oh. 2007) (holding that liability for SexSearch.com would require the court to treat SexSearch.com as the publisher of Doe's profile, which would contravene CDA 230's express provisions).

170 *Supra* Part III.A.

171 *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1172 (9th Cir. 2008) ("Roommate does not merely provide a framework that could be utilized for proper or improper purposes; rather, Roommate's work in developing the discriminatory questions, discriminatory answers and discriminatory search mechanism is directly related to the alleged illegality of the site.").

172 Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

173 *See* Jane Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 851 (W.D. Tex. 2008), *aff'd*, 528 F.3d 413 (5th Cir. 2008) ("To impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in its tracks . . . which Congress in its wisdom has decided to protect.").

174 Doe v. SexSearch, 502 F. Supp. 2d 719, 726 (N.D. Ohio 2007) (quoting Zeran v. America Online, 129 F.3d 327, 328–9 (4th Cir. 1997)).

175 *See* SexSearch, 502 F. Supp. 2d at 722 ("Plaintiff and Jane Roe engaged in consensual sexual relations . . . Jane Roe was not actually 18, but a 14-year-old child.").

176 *See id.* at 730 ("Plaintiff clearly had the ability to confirm Jane Roe's age when he met with her in person, before they had sex, yet failed to do so.").

177 *See* 47 U.S.C. § 230(b)(2) ("It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.").

178 *Supra* part III.B. The Author fully recognizes that the dating website and customer could enter into an individual signed-and-lawyered contract which some courts may hold valid, but the transaction costs associated with such a proposition are astronomical.

179 *Supra* part III.B.

180 *See, e.g.*, Matt Liebowitz, *Watch Out: Dating Website Fraud Is Running Rampant*, Business Insider (Feb. 13, 2012), http://articles.businessinsider.com/2012-02-13/news/31054222_1_okcupid-social-networking-sites-on-linepersonalswatch.

181 *See, e.g.*, State St. Bank & Trust Co. v. Signature Fin. Group, Inc., 149 F.3d 1368, 1373 (Fed. Cir. 1998) *abrogated by* In re Bilski, 545 F.3d 943 (Fed. Cir. 2008) (holding that a normally non-patentable mathematical calculation was patentable because it was run through "a machine"); *see generally* Musetta Durkee, Note, *The Truth Can Catch The Lie: The Flawed Understanding of Online Speech In In Re Anonymous Online Speakers* 26 Berkeley Tech. L.J. 773, 774 (2011) ("[C]ourts generally derive a dual narrative of the Internet: on the one hand, the Internet is a beacon of opportunity for diverse viewpoints and truly inclusive democratic dialogue; on the other, it is a harbinger of lies, characterized by anonymity and the corresponding inherent lack of accountability, at a magnitude unparalleled in human history.").

182 *See, e.g.*, Frank Greve, *Fears of Internet predators unfounded, study finds*, McClatchy Newspapers, http://www.mcclatchydc.com/2008/02/18/28029/fears-of-internet-predators-unfounded.html (Feb. 18, 2008) ("A lot of parental worries about Internet sex predators are unjustified, according to new research by a leading center that studies crimes against children. 'There's been some overreaction to the new technology, especially when it comes to the danger that strangers represent.'" (quoting Janis Wolak of the Crimes against Children Research Center at the University of New Hampshire in Durham)).

183 *See* Charlie White, *Investment Fraud Over the Internet*, The Office of the Indiana Secretary of State Securities Division, http://www.in.gov/sos/securities/files/0865-1007_InvestmentFraudBroch-FINAL_WEB.pdf ("but the anonymity of the Internet has developed an environment ripe with opportunity for scam artists to recruit you into fraudulent investments."); *Protect Yourself Against CyberFraud*, Conn. Dep't of Banking, http://www.ct.gov/dob/cwp/view.asp?a=2239&q=298088 ("The Internet is unique technology with characteristics that offer potential for certain types of fraud. As a result, scam artists are continually trying to create new schemes to take your money. . . . The Internet is also relatively anonymous, so it's important that you confidently confirm a person or entity's identity . . . .").

184 47 U.S.C. § 230(b)(1).

185 *See, e.g.*, Jana Kasperkevic, Business Insider (Feb. 28, 2012), http://articles.businessinsider.com/2012-02-28/news/31106674_1_ads-tag-lines-websites ("Two dating websites, PlentyofFish.com and True.com, are being sued for running ads featuring photos of a deceased soldier, reported The Associated Press.").

186 Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008).

187 *Id.*

188 *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 ("The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings . . . interactive computer service providers might choose to severely restrict the number and type of messages posted.").

189 *Supra* part III.C.

190 *Supra* part III.D.

191 *Supra* part III.C.

192 *Supra* part IV.D.

193 *Supra* part IV.C.

194 *See* White, *supra* note 184 and associated text.

195 The "safe harbor" would not single out dating websites, but would apply generally to all websites seeking liability protection under CDA 230.

196 47 U.S.C. § 230(b)(1).

2014 Edward F. Langs Writing Award

Essay Competition Rules

1. Awards will be given to up to six student essays, which in the opinion of the judges make the most significant contribution to the knowledge and understanding of information technology law. Factors to be taken into consideration include: originality; timeliness of the subject; depth of research; accuracy; readability; and the potential for impact on the law.

2. Essay must be original, deemed to be of publishing quality, and must not have been submitted to any other contest within the previous 12 months.

3. Essay must be typed, double spaced, at least ten pages in length, must contain proper citations listed as either endnotes or footnotes, and must have left, right, top, and bottom margins of one inch.

4. Essay must include the submitter's name, email address, mailing address, telephone number, and school attended.

5. A total of up to $3,000 in US dollars shall be divided between the award winning essays, and all rights to award winning essays shall become the property of the State Bar of Michigan.

6. The Information Technology Section of the State Bar of Michigan reserves the right to make editorial changes, and to publish award winning essays in the Section's newsletter, the Michigan IT Lawyer. (Previous issues of the Michigan IT Lawyer can be accessed at http://www.michbar.org/it/newsletters.cfm.)

7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2014, and emailed to dsyrowik@brookskushman.com.

The State of Information Technology Law—2013

By David R. Syrowik, *Brooks Kushman PC*

Introduction

Enactment of the America Invents Act was the biggest patent news of 2011, but its most comprehensive provisions were implemented September 16, 2012, and March 16, 2013. For example, one of its biggest components – the move to a first-inventor-to-file system – began on March 16th. Some of the major provisions which took effect on September 16th give patent challengers opportunities to make their cases at the Patent Office instead of in court. Four different procedures were implemented:

- *Preissuance submission of prior art*
- *Supplemental examination*
- *Interpartes review*
- *Special attack on business method patents.*

In a significant *en banc* ruling, in the *CLS Bank* case, the U.S. Court of Appeals for the Federal Circuit ruled in May of this year that computer method and computer-readable medium claims on the formulation and trading of risk management contracts are not eligible for patent protection under 35 U.S.C. § 101 as drawn to mere "abstract ideas." The court is divided 5-5 as to whether the computer system claims at issue are patent eligible.

The Supreme Court issued a ruling in a case involving a clash between two provisions of the Copyright Act, the first sale doctrine, 17 U.S.C. § 109(a), which gives the owner of a lawful copy of a creative work permission to dispose of the copy without interference from the copyright owner and Section 602(a)(1), which gives a copyright holder the right to block imports of a copy made overseas. In a 6-3 ruling, the Supreme Court held that the first sale doctrine applies to copies of works legally made overseas and imported into the United States without permission of the copyright holder.

Finally, just in time for the 2013 college football season, in the *Hart* case, the Third Circuit held in a right of publicity case that a video game maker's "realistic representation[]" of a Rutgers University quarterback is not transformative, and therefore the use of the player's likeness is not protectable expression under the First Amendment.

PATENTS – *Case Law* – U.S. Supreme Court

Bowman v. Monsanto, 86 BNA PTCJ's 118

The U.S. Supreme Court on May 13, 2013, ruled that seeds harvested from one crop are "additional copies" of Monsanto Co.'s patented invention and thus are not subject to the patent exhaustion doctrine. The decision represents a victory for Monsanto, whose patents on Roundup Ready transgenic seeds have withstood attacks from farmers for more than a decade.

PATENTS – *Case Law* – U.S. Courts of Appeal

Energy Transportation Group Inc. v. William Demant Holding, 84 BNA's PTCJ 1029

The U.S. Court of Appeals for the Federal Circuit on October 12, 2012 ruled that a patent based on computer technology in 1986 can capture later advances under the doctrine of equivalents.

Apple Inc. v. Samsung Electronics Co., 84 BNA's PTCJ 1022

The U.S. Court of Appeals for the Federal Circuit on October 11, 2012 ruled that a preliminary injunction against a Samsung smartphone is an abuse of discretion.

CLS Bank International v. Alice Corp., 84 BNA's PTCJ 990

The U.S. Court of Appeals for the Federal Circuit on October 9, 2012 agreed to rehear *en banc* a case on how to determine the patent eligibility under 35 U.S.C. § 101 of method, system, and medium claims implemented on a computer. The order vacates a split panel decision that computerized methods of eliminating risk in bank funds exchanges are patent eligible.

SanDisk Corp. v. Kingston Technology Co., 84 BNA's PTCJ 992

The U.S. Court of Appeals for the Federal Circuit on October 9, 2012 ruled that patent infringement under the doctrine of equivalents was improperly limited to exclude equivalents of subject matter cited in external references. The court overturns rulings against flash memory patent holder SanDisk Corp., correcting two interpretations of how to apply the "disclosure-dedication" rule.

***Microsoft Corp. v Motorola, Inc.*, 84 BNA's PTCJ 962**

The U.S. Court of Appeals for the Ninth Circuit on September 28, 2012 ruled that a district court properly issued a preliminary anti-suit injunction, preventing enforcement of an injunction imposed by a German court against Microsoft Corp.'s Xbox game system.

***Akamai Technologies, Inc. v. Limelight Networks Inc.; and McKesson Technologies Inc. v. Epic Systems Corp.*, 84 BNA's PTCJ 785**

The U.S. Court of Appeals of the Federal Circuit on August 31, 2012, in an *en banc*, 6-5 split, ruled that a patent owner claiming induced infringement no longer has to show a single induced entity is liable for direct infringement.

***LaserDynamics Inc. v. Quanta Computer Inc.*, 84 BNA's PTCJ 809**

The U.S. Court of Appeals for the Federal Circuit on August 3, 2012 ruled that entire market value theory is irrelevant where laptop computer demand is not driven by disc reader.

***Mirror Worlds LLC v. Apple Inc.*, 84 BNA's PTCJ 814**

The U.S. Court of Appeals for the Federal Court on September 4, 2012 affirmed a District Court reversal of a $208 million patent judgment by a jury.

***ActiveVideo Networks v. Verizon Communications Inc.*, 84 BNA's PTCJ 741**

The U.S. Court of Appeals for the Federal Circuit on August 24, 2012 ruled that Verizon remains liable for $115 million damages for infringement by its FiOS video-on-demand service, but a permanent injunction against the service is vacated.

***MagSil Corp. v. Hitachi Global Storage Technologies Inc.*, 84 BNA's PTCJ 667**

The U.S. Court of Appeals for the Federal Circuit on August 14, 2012 ruled that patent claims on "10 percent to infinity" computer performance measure not enabled.

***Bancorp Services LLC v. Sun Life Assurance Company of Canada (USA)*, 84 BNA's PTCJ 551**

The U.S. Court of Appeals for the Federal Circuit on July 26, 2012 ruled that a patent claim on managing the risk in the value of a life insurance policy is not patent eligible under 35 U.S.C. § 101. Affirming a lower court's judgment, the appeals court distinguishes post-*Bilski* rules that have addressed the patent eligibility of claims focused on an algorithm that is implemented on a computer.

***01 Communique Laboratory Inc. v. Log Me In Inc.*, 84 BNA's PTCJ 561**

The U.S. Court of Appeals for the Federal Circuit on July 31, 2012 ruled that patent's internet-based software functions can be distributed over multiple computers.

***CLS Bank International v. Alice Corp.*, 84 BNA's PTCJ 391**

The U.S. Court of Appeals for the Federal Circuit on July 9, 2012 in a split decision, ruled that computerized methods of eliminating risk in bank funds exchanges are patent eligible. Reversing a district court ruling, the majority analyzes the "inventive concept" – a term introduced by the Supreme Court's recent decision in *Mayo v. Prometheus* – of the patent claims asserted by looking at the claims as a whole.

***In re Mouttet*, 84 BNA's PTCJ 354**

The U.S. Court of Appeals for the Federal Circuit on June 26, 2012 ruled that a nanoprocessor system was obvious as mere substitution of nanoscale materials.

***In re Ranbus Inc.*, 103 USPQ2d 1865**

The U.S. Court of Appeals for the Federal Circuit on August 15, 2012 ruled that invention of claim directed to method of operation of synchronous "memory device" was anticipated by "memory module" disclosed in prior art reference manual, since claimed "memory device" can contain more than one chip, and may contain controller that provides logic necessary to receive and output specific data but does not function like central processing unit, since "memory control unit" in prior art memory module provided necessary logic, since bus controller of prior art device was clearly outside memory module, thereby satisfying claim's requirement that memory device receive block size request from bus controller, and since there is consequently no principled way to distinguish claim at issue from prior art memory module.

***Voter Verified Inc. v. Premier Election Solutions Inc.*, 85 BNA's PTCJ 36**

The U.S. Court of Appeals for the Federal Circuit on November 5, 2012 ruled that automated voting machine makers do not infringe a patent that was applied for a month after the Florida paper ballots controversy in 2000. The court rules

that an article in an online journal is "publicly accessible" as qualifying prior art, even if commercial search engines are unaware of it, so long as the journal is known by persons of skill in the art and it has its own search tool.

ePlus Inc. v. Lawson Software Inc., 85 BNA's PTCJ 131

The U.S. Court of Appeals for the Federal Circuit on November 21, 2012 ruled that a patent system claim is indefinite for failure to provide corresponding hardware, code, or algorithm to support a "mean" "for processing" limitation.

Soverain Software v. Newegg, 85 BNA's PTCJ 409

The U.S. Court of Appeals for the Federal Circuit on January 22, 2013 ruled that a pre-internet system for computer-based shopping rendered internet e-commerce claims obvious. Reversing a lower court's validity ruling, the appeals court takes elements of the CompuServe Mall, which existed in the late 1980s, and adds updates based on World Wide Web conventions that would be obvious to a person of skill in computer science.

Parallel Networks v. Abercrombie & Fitch, 85 BNA's PTCJ 410

The U.S. Court of Appeals for the Federal Circuit on January 16, 2013 ruled that the owner of a website applet-delivery patent must live with its choice "to pursue a theory that allowed it to accuse a larger number of defendants," and so cannot modify its arguments based on a claim construction that defeated its infringement complaint. The court also affirms a decision not allow an amended complaint in light of a "hardly unanticipated" claim construction.

Technology Patents LLC v. T-Mobile (UK) Ltd., 105 USPQ2d 1257

The U.S. Court of Appeals for the Federal Circuit on November 17, 2012 affirmed that grant of summary judgment that defendant software providers do not infringe certain claims of patent for global paging system using internet since plaintiff has not produced sufficient evidence that accused paging systems are even capable of meeting disputed limitations of claims in question; however, summary judgment of noninfringement as to remaining asserted claims is vacated and remanded, since district court based judgment on its finding that claims require multiple actors, but claims do not present issue of "joint" or "divided" infringement.

Function Media v. Google, 85 BNA's PTCJ 545

The U.S. Court of Appeals for the Federal Circuit on February 13, 2013 ruled that Google does not infringe website advertising patents that implicate its AdWords and AdSense products.

In re Hartman, 85 BNA's PTCJ 676

The U.S. Court of Appeals for the Federal Circuit on March 8, 2013 in a non-precedential ruling affirmed the rejection of claims under 35 U.S.C. § 112 to inventing the Internet.

Versata Software v. SAP America, 86 BNA's PTCJ 13

The U.S. Court of Appeals for the Federal Circuit on May 1, 2013 ruled that the record supported a $345 million award for software patent infringement by SAP America Inc. in an unusual situation in which a defendant succeeded in getting a second damages trial, but the second jury increased the award by more than $200 million.

Ceats Inc. v. Continental Airlines Inc., 86 BNA's PTCJ 18

The U.S. Court of Appeals for the Federal Circuit on April 26, 2013 in a non-precedential opinion upheld the ruling that a patent on online airline and venue seat selection as anticipated by Expedia.

CLS Bank International v. Alice Corp., 86 BNA's PTCJ 120

An *en banc* U.S. Court of Appeals for the Federal Circuit on May 10, 2013 ruled that computer method and computer-readable medium claims on the formulation and trading of risk management contracts are not eligible for patent protection under 35 U.S.C. § 101 as drawn to mere "abstract ideas." The court is divided 5-5 as to whether the computer system claims at issue are patent eligible.

Brilliant Instruments Inc. v. GuideTech LLC, 105 USPQ2d 1879

The U.S. Court of Appeals for the Federal Circuit on February 20, 2013 ruled that accused time interval analyzers, which detect timing errors in digital signals of high-speed microprocessors, do not literally infringe asserted claims; however, patentee's theory of infringement by equivalents does not vitiate requirement that "first current circuit" and "capacitor" recited in claims be separate elements, and genuine issue of material fact exists as to whether accused products infringe under doctrine of equivalents.

***Move Inc. v. Real Estate Alliance Ltd.*, 105 USPQ2d 1948**

The U.S. Court of Appeals for the Federal Circuit on March 4, 2013 ruled that accused system does not directly infringe claim for computerized method of locating real estate properties; however, liability for induced infringement may arise when steps of method claim are performed by more than one entity, and district court erred by not conducting indirect infringement analysis.

***Speedtrack Inc. v. Endeca Technologies Inc.*, 106 USPQ2d 1442**

The U.S. Court of Appeals for the Federal Circuit on April 16, 2013 in an unpublished opinion ruled that district court in action alleging infringement of patent for computer filing system in which data storage is linked to assigned categories, did not abuse its discretion in holding that defendant was not judicially estopped from arguing that disputed claim term "category description" cannot consist solely of numerical identifiers, despite seemingly contrary position taken by defendant in requesting reexamination by U.S. Patent and Trademark Office.

***In re Bayse*, 86 BNA's PTCJ 342**

The U.S. Court of Appeals for the Federal Circuit on June 5, 2013 in an opinion designated as non-precedential ruled that an Internet-based patent application on getting cash loan at an ATM when funds were insufficient was obvious.

PATENTS – *Case Law* – U.S. District Courts

***Apple Inc. v. Samsung Electronics Co.*, 84 BNA's PTCJ 739**

A jury in the U.S. District Court for the Northern District of California on August 24, 2012 awarded nearly $1.05 billion to Apple after it finds utility and design patent infringement by 25 distinct cell phone and three tablet computer devices made by Samsung.

***Apple Inc. v. Samsung Electronics Co.*, 84 BNA's PTCJ 416**

The U.S. District Court for the Northern District of California on July 1, 2012 granted Apple a preliminary injunction when it stated that Samsung Nexus Smartphone likely infringes.

***Apple Inc. v. Samsung Electronics Co.*, 84 BNA's PTCJ 338**

The U.S. District Court for the Northern District of California on June 26, 2012 ordered a preliminary injunction barring Samsung Electronics Co. from making, using, offering to sell, selling, or importing the Galaxy Tab 10.1 tablet computer in the United States. The decision follows a ruling by the Federal Circuit denying Apple Inc's request for an injunction against Samsung's Android-based smart phones but leaving the tablet injunction decision up to District Court Judge Lucy H. Koh.

***Apple Inc v. Motorola Inc.*, 84 BNA's PTCJ 349**

The U.S. District Court for the Northern District of Illinois on June 22, 2012 dismissed the Apple – Motorola smartphone patent fight for lack of remedy.

***Microsoft Corp. v. Motorola Inc.*, 103 USPQ2d 1235**

The U.S. District Court for the Western District of Washington on February 27, 2012 granted plaintiff summary judgment that defendant patentees entered into binding contracts with international standards-setting organizations requiring defendants to license, on reasonably nondiscriminatory terms and conditions, patents that have been declared "essential" to practicing standards for interoperability of computing devices; however, summary judgment is denied on questions of whether defendants' initial license offer, not just final negotiated license, must be on RAND terms, and whether defendants' offers to plaintiff breached defendants' RAND obligations.

***Microsoft Corp v. Motorola Inc.*, 84 BNA's PTCJ 1023**

The U.S. District Court for the Western District of Washington on October 10, 2012 ruled that Motorola Inc. must agree to license standard-essential patents to Microsoft Corp., and if the parties cannot come to an agreement, a federal court will force one.

***IP Engine Inc. v. AOL Inc.*, 85 BNA's PTCJ 107**

A jury in proceedings in the U.S. District Court for the Eastern District of Virginia on November 6, 2012 finds Google and AOL infringe ad tracking patents 6,314,420 and 6,775,664, and awards firm $30 million.

***SmartGene v. Advanced Biological Laboratories*, 85 BNA's PTCJ 348**

The U.S. District Court for the District of Columbia ruled that *Mayo v. Prometheus* had no effect on whether a computer-based medical expert system is patent eligible, rejecting a patent owner's motion for reconsideration of her earlier decision in the case.

Apple Inc. v. Samsung Electronics Co.,
85 BNA's PTCJ 316

The U.S. District Court for the Northern District of California on December 17, 2012 ruled that new evidence proffered by Apple to justify a request for a permanent injunction against Samsung smartphones is insufficient. Following a jury verdict favoring Apple, the court denies Apple's motion for a permanent injunction and again finds lacking the company's evidence intended to show a causal nexus between Samsung's infringement and consumer demand. According to the court, prior rulings set the standard that Apple bears the burden of showing that any identified sales of infringing Samsung phones occurred as a result of Samsung's incorporation of the infringing feature.

Apple v. Samsung Electronics, **85 BNA's PTCJ 441**

The U.S. District Court for the Western District of California on January 29, 2013 ruled that a jury's $1 billion damages award against Samsung for infringing Apple Inc.'s smartphone patents is supported by the record and therefore Samsung is not entitled to either a judgment as a matter of law to overturn the verdict, or to new trial. The court does, however, grant Samsung judgment as a matter of law that its patent infringement is not willful.

Via Vadis Controlling G.m.b.H. v. Skype, Inc.,
85 BNA's PTCJ 585

The U.S. District Court for the District of Delaware on February 21, 2013 ruled that Skype is not compelled to disclose its source code in patent infringement litigation in Germany and Luxembourg.

Microsoft v. Motorola, **86 BNA's PTCJ 19**

The U.S. District Court for the Western District of Washington on April 25, 2013 ruled that Motorola Inc.'s offer to Microsoft Corp. to license patents essential to two widespread computing standards is dramatically higher than the companies would have agreed to in a typical licensing negotiation. Consequently, the Court said that Motorola's patents were valued up to 76¢, not $6.00.

PATENTS – *Case Law* – International Trade Commission (ITC)

In the Matter of Certain Mobile Telephones and Wireless Communication Devices Featuring Digital Cameras and Components Thereof, **84 BNA's PTCJ 510**

The International Trade Commission on July 20, 2012 ruled that Apple Inc. and Research in Motion Ltd. escape liability for patent infringement because the sole patent claim asserted by Eastman Kodak Co. is found invalid by the International Trade Commission. The decision is a temporary blow to Kodak, which is trying to emerge from bankruptcy in part by auctioning its patents.

In the Matter of Certain Electronic Devices, Including Wireless Communication Devices
86 BNA's PTCJ 277

The International Trade Commission on June 4, 2013 issued an exclusion order barring Apple from importing older iPhone and iPad models used on AT&T network.

PATENTS – *Case Law* – U.S. Patent and Trademark Office

SAP America Inc. v. Versata Development Group Inc.,
86 BNA's PTCJ 335

The Patent Trial and Appeal Board on June 11, 2013 issued its first decision on a post-issuance patent challenge enabled by the America Invents Act. The board holds that the challenged claims of a "covered business method" patent were ineligible for a patent under 35 U.S.C. § 101.

PATENT/ANTITRUST/BANKRUPTCY – *Case Law* - U.S. Court of Appeals

Eatoni Ergonomics Inc. v. Research in Motion Corp.,
84 BNA's PTCJ 355

The U.S. Court of Appeals for the Second Circuit on June 21, 2012 ruled that RIM didn't breach settlement agreement, violate Sherman Act.

PATENT/ANTITRUST/BANKRUPTCY – *Case Law* - U.S. District Court

PNY Technologies Inc. v. SanDisk Corp.,
103 USPQ2d 1109

The U.S. District Court for the Northern District of California on April 20, 2012 ruled that plaintiff has made sufficient showing in complaint that defendant has monopoly power over upstream market for flash memory technology, since plaintiff alleges that defendant owns 100 percent of flash memory technology patents; however, plaintiff has failed to state claims for monopolization or attempted monopolization under Sherman Act's Section 2, or for conspiracy in restraint of trade under Section 1.

***Cascades Computer Innovation LLC v. RPX Corp.,* 85 BNA's PTCJ 458**

The U.S. District Court for the Northern District of California on January 24, 2013 a patent troll suffers dismissal of Sherman Act claims of android device makers' boycott.

COPYRIGHTS – *Case Law* - U.S. Supreme Court

***Kirtsaeng d/b/a Bluechristine 99 v. John Wiley & Sons Inc.,* 85 BNA's PTCJ 695**

The U.S. Supreme Court on March 19, 2013 in a 6-3 ruling held that the first sale doctrine, as codified in the federal copyright statute, applies to copies of works legally made overseas and imported into the United States without the permission of the copyright holder.

COPYRIGHTS – *Case Law* - U.S. Court of Appeal

***Capitol Records Inc. v. Thomas-Rasset,* 84 BNA's PTCJ 792**

The U.S. Court of Appeals for the Eighth Circuit on September 11, 2012 ruled that the Due Process Clause does not bar a Copyright Act statutory damages award of $222,000 - $9,250 for each of 24 songs – that a jury awarded against an individual who infringed the songs over the internet file-sharing program.

***WPIX Inc. v. iVi Inc.,* 84 BNA's PTCJ 740**

The U.S. Court of Appeals for the Second Circuit on August 27, 2012 affirmed that a paid online service that streams broadcast content live to subscribers and offers a remote digital video recording service is not a "cable system" entitled to a compulsory license under the Copyright Act.

***GlobeRanger Corp. v. Software AG,* 84 BNA's PTCJ 713**

The U.S. Court of Appeals for the Fifth Circuit on August 17, 2012 held that business practices suggested by software are beyond scope of copyright protection.

***Flava Works Inc. v. Gunter d/b/a myVidster.com,* 84 BNA's PTCJ 622**

The U.S. Court of Appeals for the Seventh Circuit on August 2, 2012 ruled that website users' links to infringing uploads unlikely to create copyright liability for site.

***Society of the Holy Transfiguration Monastery Inc. v. Archbishop Gregory of Denver, Colo.,* 103USPQ2d 1585**

The U.S. Court of Appeals for the First Circuit on August 2, 2012 ruled that plaintiff monastery established that it owns valid copyrights in translations of religious texts, and that copies of texts available on defendant's website are substantially similar to plaintiff's works, and grant of summary judgment of infringement is therefore affirmed.

***St. Luke's Cataract and Laser Institute v. Zurich American Insurance,* 85 BNA's PTCJ 509**

The U.S. Court of Appeals for the Eleventh Circuit on February 7, 2013 ruled that an insurance policy that excludes coverage for advertising claims based on the use of another's name or product in the insured party's email address, domain name, or metatags does not preclude coverage for a copyright infringement claim based on a website.

***Columbia Pictures Industries Inc. v. Fung,* 85 BNA's PTCJ 748**

The U.S. Court of Appeals for the Ninth Circuit on March 21, 2013 held that a BitTorrent website operator's invitations to users to upload specific infringing content supplied the intent necessary to hold him culpable for users' infringements under an inducement of copyright infringement theory.

***Luvdarts v. AT&T Mobility,* 85 BNA's PTCJ 751**

The U.S. Court of Appeals for the Ninth Circuit on March 25, 2013 held that AT&T, Verizon, Sprint Nextel, and T-Mobile not liable for copyright infringement based on their subscribers' alleged unauthorized sharing of copyrighted content on the carriers' multimedia messaging services.

WNET *v. Aereo Inc.,* 85 BNA's PTCJ 799

The U.S. Court of Appeals for the Second Circuit on April 1, 2013 ruled that Aereo Inc.'s use of individual antennas allowing subscribers to watch television programs online at nearly the same time as they are being broadcast, does not constitute a public performance under *Cablevision*.

COPYRIGHTS – *Case Law* - U.S. District Courts

***McGraw-Hill Cos. v. Google Inc.,*84 BNA's PTCJ 989**

The U.S. District Court for the Southern District of New York on October 4, 2012 one of the parties in a long-running dispute over Google Inc.'s mass digitization of books announces that it is settling its claim with Google. The Association of American

Publishers and Google release a statement that they have agreed to settle their now seven-year-old dispute.

Third Degree Films v. Doe, 84 BNA's PTCJ 996

The U.S. District Court for the District of Massachusetts on October 2, 2012 ruled that joinder in BitTorrent cases "technically" okay but inappropriate due to potential abuse.

Pacific Stock v. MacArthur & Co., 84 BNA's PTCJ 1003

The U.S. District Court for the District of Hawaii on October 2, 2012 ruled that Web magazine's removal of copyright notice, adding own, warrants maximum DMCA damages.

Spry Fox LLC v. Lolapps Inc., 84 BNA's PTCJ 965

The U.S. District Court for the Western District of Washington on September 18, 2012 ruled that a video game maker's copyright infringement claims against a competitor survive dismissal.

AF Holdings LLC v. Doe, 84 BNA's PTCJ 820

The U.S. District Court for the Northern District of California on September 4, 2012 ruled that the Copyright Act preempts negligence lawsuit alleging failure to secure wireless network.

Sony BMG Music Entertainment v. Tenenbaum, 103 USPQ2d 1902

The U.S. District Court for the District of Massachusetts on August 23, 2012 ruled that jury award of $22,500 per infringement, for total damages award of $675,000, in action against defendant based on his file-sharing of music recordings, does not offend due process, since award is neither "wholly disproportioned to the offense" nor "obviously unreasonable", given deference afforded to U.S. Congress in offering and establishing statutory damages as option to collection of actual damages, and in increasing penalties for willful infringement, and in view of defendant's particular behavior and fact that award not only is within range for willful infringement, but also below limit for non-willful infringement.

Discount Video Center Inc. v. Does 1-29, 103 USPQ2d 1759

The U.S. District Court for the District of Massachusetts on July 5, 2012 denied a motion to quash subpoena requesting identities of 29 Doe defendants from their respective internet service providers in case arising from alleged trading of copyrighted work in related transactions using BitTorrent software.

WNET v. Aereo Inc., 102 USPQ2d

The U.S. District Court for the Southern District of New York on May 18, 2012 ruled that text and structure of preemption statute, 17 U.S.C. § 301(a), suggest that Copyright Act preempts unfair competition claim asserted by television production, distribution, and transmission companies alleging that defendant's internet-based broadcast television streaming service "unfairly exploit(s) Plaintiffs' property interests in their audiovisual works" for defendant's commercial benefit, even though defendant's service involves private performances that are not actionable under Copyright Act.

Branca v. Mann, 84 BNA's PTCJ 716

The U.S. District Court for the Central District of California on August 10, 2012 ruled that Michael Jackson's estate is not precluded from pursuing claims against "Vault" website.

American Broadcasting Cos. v. Aereo Inc., 84 BNA's PTCJ 456

The U.S. District Court for the Southern District of New York on July 11, 2012 ruled that the system that Aereo Inc. uses to allow its customers to watch and record television broadcasts is "materially identical" to the system used in *Cablevision*, and thus the Second Circuit's determination that the Cablevision device does not transmit the broadcast precludes an issuance of a preliminary injunction against Aereo.

Shutterfly Inc. v. Forever Arts Inc., 84 BNA's PTCJ 483

The U.S. District Court for the Northern District of California on July 13, 2012 granted Shutterfly a TRO against former employee for alleged theft of copyrighted source code.

Siniouguine v. Mediachase Ltd., 84 BNA's PTCJ 420

The U.S. District Court for the Central District of California on June 11, 2012 ruled that a software programmer is employee even with gaps in receipts of regular salary.

Northland Family Planning Clinic Inc. v. Center for Bio-Ethical Reform, 84 BNA's PTCJ 358

The U.S. District Court for the Central District of California on June 15, 2012 ruled anti-abortion websites' use of pro-choice film was fair use of parody under Section 107.

Tetrix Holding LLC v. XIO Interactive Inc., 103 USPQ2d 1959

The U.S. District Court for the District of New Jersey on May 30, 2012 ruled that principle that patents and copyrights protect distinct aspects of intellectual property does not mean that any and all expression related to rule or function of video game falls outside protection of copyright law, since expression is unprotected only if it is integral to or inseparable from idea or function under doctrines of merger or scenes à faire, and expression of "method of operation" is copyrightable if it is distinguished from method itself and is not essential to its operation; in present case, defendants' accused video puzzle game is substantially similar to plaintiff's copyrighted game with regard to design and movement of playing pieces, as well as other discrete copyrightable elements.

Xcentric Ventures LLC v. Mediolex Ltd., 85 BNA's PTCJ 19

The U.S. District Court for the Southern District of Arizona on October 24, 2012 ruled that a website operator that encouraged visitors to post negative reviews on a rival gripe site is not contributorily liable for those users' alleged infringement of the rival site's copyrights.

Malibu Media LLC v. Doe, 85 BNA's PTCJ 189

The U.S. District Court for the Southern District of New York on November 30, 2012 ruled that pornography file-sharing defendant allowed to proceed unnamed due to privacy issues.

Fox Television Stations Inc. v. BarryDriller Content Systems PLC, 85 BNA's PTCJ 305

The U.S. District Court for the Central District of California on December 27, 2012 ruled that a service that purportedly allows subscribers to stream broadcast television content to their computers and mobile devices via mini-antennas infringes content industry copyrights. The opinion is in tension with a New York district court's ruling in July that found a similar device non-infringing.

John Wiley & Sons, Inc. v. Williams, 104 USPQ2d 1709

The U.S. District Court for the Southern District of New York on November 5, 2012 granted default judgment to plaintiff alleging illegal reproduction and distribution of copyrighted "For Dummies" books over internet using "BitTorrent" file-sharing protocol against defendants who have not entered appearance in case, and is awarded $3,000 in statutory damages from each defendant.

Aerosoft GMBH v. Does 1-50, 104 USPQ2d 1697

The U.S. District Court for the Southern District of Florida on October 23, 2012 stated that plaintiff's permissive joinder of 50 Doe defendants, in action alleging illegal reproduction and distribution of copyrighted video game over internet using "BitTorrent" file-sharing protocol, is improper under Fed.R.Civ.P. 20(a)(2); defendants' decision to obtain BitTorrent software and download same copyrighted work does not, in and of itself, constitute "same transaction, occurrence, or series of transactions or occurrences."

Authors Guild Inc. v. HathiTrust, 104 USPQ2d 1659

The U.S. District Court for the Southern District of New York on October 10, 2012 ruled that plaintiff domestic associational organizations do not have statutory standing to bring copyright infringement action, on behalf of their members, challenging universities' agreements with internet search engine that allow search engine to create digital copies of works in universities' libraries, since case law interpreting 17 U.S.C. § 501(b) indicates that Copyright Act does not permit copyright holders to have others sue on their behalf.

Ardis Health LLC v. Nankivell, 104 USPQ2d 1856

The U.S. District Court for the Southern District of New York on October 23, 2012 ruled that defendant's state-law claim alleging conversion of website is preempted by federal copyright law, since conversion claims are routinely held to be not quantitatively different from copyright claims, since defendant, by alleging that she "created" website, including its "design" and "distinctive look," and that plaintiffs and third-party defendant exercised "unauthorized dominion" over work and presented it to public as their own, asserts claim that falls squarely within general ambit of federal copyright law, and since claim does not contain "extra element" that would protect conversion claim from preemption.

Routt v. Amazon.com Inc., 105 USPQ2nd 1089

The U.S. District Court for the Western District of Washington on November 30, 2012 ruled that plaintiff has failed to state plausible claim that defendant online retailer is vicariously liable for copyright infringement allegedly committed by participants in defendant's "associates program" since vicarious liability requires some version of agency relationship, and plaintiff has not stated plausible claim that associates are not "solely responsible" for content of their websites, as stated in defendant's "associates agreement."

***Ingenuity 13 L.L.C. v. Doe,* 85 BNA's PTCJ 516**

The U.S. District Court for the Central District of California on February 7, 2013 ruled that unsupported BitTorrent pleadings provoke sanctions hearing for plaintiff's counsel.

***Agence France-Presse v. Morel,* 85 BNA's PTCJ 416**

The U.S. District Court for the Southern District of New York on January 14, 2013 ruled that the terms of service of Twitter's microblogging service do not support the argument that posting images on Twitter grants third parties an unrestricted license to re-use those images.

***Fox Broadcasting Co. v. Dish Network LLC,* 105 USPQ2d 1541**

The U.S. District Court for the Central District of California on November 7, 2012 ruled that plaintiff owners of copyrights in network television programming have failed to establish likelihood of success on merits of their claims that defendant satellite television service is liable for direct, contributory, or vicarious infringement of plaintiffs' copyrights by making available to subscribers set-top boxes that can record broadcast network programming, since evidence does not suggest that consumers use recording feature for anything other than time-shifting in their homes or on mobile devices, which has been held to be legitimate, noninfringing practice.

***AF Holdings LLC v. Doe,* 105 USPQ2d 1490**

The U.S. District Court for the Northern District of California on January 7, 2013 ruled that plaintiff, in action in which prior complaints alleged only negligence against defendant, is denied leave to file second amended complaint alleging direct and contributory infringement against same defendant by means of online file sharing using "BitTorrent" transfer protocol.

***Metabyte Inc. v. NVIDIA Corp.,* 106 USPQ2d 1931**

The U.S. District Court for the Northern District of California on April 22, 2013 ruled plaintiff's claim for unfair business practices under California law is preempted by Copyright Act, since claim alleges that defendant company created and sold products that were substantially similar to plaintiff's copyrighted software, and that products included plaintiff's proprietary information by way of direct copies and derivative works acquired through alleged theft and copying of software, and since reproduction of copyrighted works, preparation of derivative works, and distribution of copies to public are all rights granted under Copyright Act.

***Capitol Records L.L.C. v. ReDigi Inc.,* 85 BNA's PTCJ 802**

The U.S. District Court for the Southern District of New York on March 30, 2013 held that the operators of an online music marketplace that allows users to buy and sell their legally downloaded music tracks are liable for direct and secondary copyright infringement. The court rejects ReDigi Inc.'s argument that the resale of the digital tracks is protected by the first-sale doctrine.

***Faktor v. Yahoo! Inc.,* 85 BNA's PTCJ 942**

The U.S. District Court for the Southern District of New York on April 16, 2013 ruled that the Copyright Act preempts Yahoo! idea-stealing suit.

***Football Association Premier League v. YouTube,* 86 BNA's PTCJ 165**

The U.S. District Court for the Southern District of New York on May 15, 2013 stated that copyright claim are "poor candidates for class-action treatment," as it denies class certification to a worldwide group of plaintiffs claiming their works had been uploaded to YouTube Inc. without their consent.

***David v. CBS Ineractive Inc.,* 106 USPQ2d 1773**

The U.S. District Court for the Central District of California on February 19, 2013 denied plaintiff recording artists and copyright owners preliminary injunction in action alleging that defendants induced infringement of copyrights through use of peer-to-peer file sharing software, since there is no evidence of any ongoing distribution of any file-sharing software by defendants with object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement.

***Design Data Corp. v. Unigate Enterprise Inc.,* 105 USPQ2d 1718**

The U.S. District Court for the Northern District of California on January 29, 2013 ruled that a claim for restitution under theory of breach of contract implied in law/quantum meruit, based on alleged unauthorized copying and use of plaintiff's copyrighted structural steel detailing software, is pre-empted by federal copyright law, since claim based on implied in-law contract includes no "extra element" in addition to defendant's unauthorized use of copyrighted work, and is therefore equivalent to rights protected by Copyright Act.

***AF Holdings LLC v. Rogers,* 105 USPQ2d 1723**

The U.S. District Court for the Southern District of California on January 29, 2013 ruled that plaintiff's claim alleging that defendant was negligent in either failing to secure his internet connection or permitting someone to use his internet connection, resulting in infringement of copyright in plaintiff's video, is preempted by Copyright Act, since claim is equivalent to contributory infringement claim to extent it rests on theory of knowing facilitation of infringement; claim also fails to extent it is based on purported "duty" to properly secure internet connection or to monitor use of secured connection by others.

***Associated Press v. Meltwater U.S. Holdings Inc.,* 106 USPQ2d 1509**

The U.S. District Court for the Southern District of New York on March 21, 2013 ruled that purpose and character of use of copyrighted news articles weighs against finding of fair use by defendant online news monitoring service, which uses computer program to "scrape" articles and provide excerpts thereof to daily reports sent to subscribers, and plaintiff news cooperative is granted summary judgment on fair-use defense.

COPYRIGHTS/CRIMINAL – *Case Law* - U.S. Court of Appeals

***United States v. Fair,* 85 BNA's PTCJ 99**

The U.S. Court of Appeals for the District of Columbia on November 9, 2012 ruled that the district court erred when it ordered a defendant who sold pirated software on eBay to pay as restitution the defendant's profit instead of the victim's lost profits.

COPYRIGHTS/CRIMINAL – *Case Law* - U.S. District Court

***United States v. Dotcom,* 84 BNA's PTCJ 1037**

The U.S. District Court for the Eastern District of Virginia on October 5, 2012 ruled in a file sharing case that a criminal summons may be mailed to Megaupload's alter ego.

***United States v. Blanco,* 85 BNA's PTCJ 43**

The U.S. Attorney acting in the U.S. District Court for the Northern District of California on October 31, 2012 said that a Northern California man is sentenced to 27 months in prison and ordered to pay $200,000 restitution after his guilty plea to criminal copyright infringement in a case that resulted in the seizure of more than 20,000 counterfeit DVDs.

***United States v. Sheikh,* 85 BNA's PTCJ 144**

A Baltimore man, in the U.S. District for the District of Maryland on November 19, 2012 pleaded guilty to mass reproduction and distribution of popular software programs.

***United States v. Newsome,* 85 BNA's PTCJ 248**

The U.S. District Court for the Eastern District of Virginia on December 3, 2012 sentenced a website owner/operator to 11 months for selling copies of pirated software.

***United States v. Ferrer,* 85 BNA's PTCJ 918**

The U.S. District Court for the Eastern District of Virginia on April 10, 2013 sentenced a member of a major movie piracy group to 23 months in prison.

COPYRIGHTS/DMCA – *Case Law* – U.S. Court of Appeals

***UMG Recordings Inc. v. Shelter Capital Partners L.L.C.,* 85 BNA's PTCJ 698**

The U.S. Court of Appeals for the Ninth Circuit on March 14, 2013 ruled that actual knowledge and "red flag" knowledge of infringement by users of an online service are two ways that a service provider can lose protection of a safe harbor, but both require knowledge of specific instances of infringement, not a generalized awareness that infringement might be taking place, superseding a 2011 opinion for reconsideration in light of another federal appeals court's ruling on similar issues.

COPYRIGHTS/DMCA – *Case Law* – U.S. District Courts

***Obodai d/b/a Heptad v. Demand Media Inc.,* 84 BNA's PTCJ 361**

The U.S. District Court for the Southern District of New York on June 12, 2012 held that keyword ad placement, website metrics don't yield notice of website's infringement.

***Lenz v. Universal Music Corp.,* 105 USPQ2d 1635**

The U.S. District Court for the Northern District of California on January 24, 2013 ruled that defendants copyright owners, in action alleging that they made material misrepresentations in issuing Digital Millennium Copyright Act "takedown" notice that caused plaintiff's home video to be removed from video-hosting website, have failed to establish that plaintiff is precluded from recovering any damages under 17 U.S.C. § 512(f), since plaintiff could potentially recover minimal expenses, such as costs of electricity used to power her computer while attempting to have her video

reinstated, even though such costs are not substantial economic damages.

***Tuteur v. Crosley-Curcuran*, 85 BNA's PTCJ 916**

The U.S. District Court for the District of Massachusetts on April 10, 2013 ruled that a blogger's DMCA challenge to rival's posting of her gesture photo not actionable.

***Viacom International Inc. v. YouTube Inc.*, 85 BNA's PTCJ 975**

The U.S. District Court for the Southern District of New York on April 18, 2013 held that an internet service provider only forfeits protection under the Digital Millennium Copyright Act if it "influence(s) or participate(s)" in infringement activities perpetrated by its users. The court says that YouTube Inc.'s general awareness of infringing clips on its servers does not impose upon the company an affirmative duty to search for and remove infringing material.

***Perfect 10 Inc. v. Yandex N.V.*, 86 BNA's PTCJ 62**

The U.S. District Court for the Northern District of California on May 7, 2013 ruled that DMCA takedown notices need not be in most convenient forms for a service provider in order to comply with Federal law.

***Capitol Records, Inc. v. MP3tunes L.L.C.*, 86 BNA's PTCJ 114**

The U.S. District Court for the Southern District of New York on May 14, 2013 "reluctantly" agrees to reconsider MP3tunes' red flag liability under DMCA.

COPYRIGHTS/DMCA – *Case Law* – State Courts – New York

***UMG Recordings v. Escape Media Group*, 86 BNA's PTCJ 9**

The New York Supreme Court, Appellate Division on April 23, 2013 ruled that the Digital Millennium Copyright Act's safe harbor provision does not apply to internet service providers' user-directed infringement of sound recordings made before February 15, 1972.

COPYRIGHTS/JURISDICTION – *Case Law* – U.S. District Court

***Penguin Group (USA) Inc. v. American Buddha*, 85 BNA's PTCJ 662**

The U.S. District Court for the Southern District of New York on March 7, 2013 ruled that failure to show "substantial revenue" dooms copyright infringement claim against website for lack of personal jurisdiction.

***Rhapsody Solutions LLC v. Cryogenic Vessel Alternatives, Inc.*, 85 BNA's PTCJ 671**

The U.S. District Court for the Southern District of Texas on March 5, 2013 ruled that a company subject to jurisdiction in Texas for accessing server to evaluate program.

COPYRIGHTS/DISCOVERY – *Case Law* – U.S. District Court

***Obodai v. Indeed Inc.*, 85 BNA's PTCJ 861**

The U.S. District Court for the Northern District of California on March 21, 2013 ruled that a defendant in a copyright infringement proceeding may subpoena from Google Inc. nine months' worth of internet protocol address information linked to a plaintiff's Gmail account.

TRADEMARKS – *Case Law* – U.S. Supreme Court

***Already LLC v Nike Inc.*, 85 BNA's PTCJ 341**

The U.S. Supreme Court on January 9, 2013 affirmed, in a unanimous ruling, that Nike Inc.'s covenant not to sue a competitor for trademark infringement, delivered after Nike has filed an infringement lawsuit against the competitor and even then only after the competitor has filed a counterclaim seeking a cancellation of Nike's mark, divested the federal district court of Article III jurisdiction.

TRADEMARKS – *Case Law* – U.S. Court of Appeals

***Gibson v. Texas Department of Insurance*, 104 USPQ2d 2029**

The U.S. Court of Appeals for the Fifth Circuit on October 30, 2012 ruled that plaintiff sufficiently pleaded as-applied challenge to Tex. Lab. Code § 419.002, which prohibits parties from using, for advertising purposes, term "Texas" in combination with "workers' compensation" or "workers' comp." since Texas government has not shown that plaintiff's "texas-workerscomplaw.com" domain name is inherently misleading, and domain name is entitled to some First Amendment protection.

***Community Trust Bancorp Inc. v. Community Trust Financial Corp.*, 84 BNA's PTCJ 747**

The U.S. Court of Appeals for the Sixth Circuit on August 23, 2012 ruled that a bank with only a handful of customers

in Kentucky could not be sued for trademark infringement in the state based on those customers' use of its banking website.

***Lens.com Inc. v. 1-800 Contacts Inc.*, 84 BNA's PTCJ 614**

The U.S. Court of Appeals for the Federal Circuit on August 3, 2012 ruled that use of software to sell goods online does not support finding that it is in commerce.

***Papa Ads LLC v. Gatehouse Media Inc.*, 104 USPQ2d 1238**

The U.S. Court of Appeals for the Sixth Circuit on June 13, 2012 affirmed a summary judgment that plaintiff's descriptive mark "iShopStark.com" lacks secondary meaning in action alleging that mark, which is domain name for website that promotes goods and services of businesses in Stark County, Ohio, is infringed by defendants' "ShopNStark.com" domain name for competing website.

TRADEMARKS – *Case Law* – U.S. District Court

***CollegeSource Inc. v. AcademyOne Inc.*, 85 BNA's PTCJ 17**

The U.S. District Court for the Eastern District of Pennsylvania on October 25, 2012 ruled that an online educational services company's purchase of a competitor's marks to trigger web advertisements was not infringing.

***AK Metals v. Norman Industrial Materials*, 85 BNA's PTCJ 480**

The U.S. District Court for the Southern District of California on January 31, 2013 ruled that a business that used a competitor's mark in key word ads, indicating that the sponsored result was "related to" the user's search terms, likely did not infringe the competitor's mark.

***Deckers Outdoor v. Doe*, 85 BNA's PTCJ 418**

The U.S. District Court for the Northern District of Illinois on January 16, 2013 ruled that the sale of counterfeit Ugg products through domain names incorporating the mark is likely to cause consumer confusion and irreparable harm to the brand.

***Rovio Entertainment Ltd. v. Royal Plush Toys Inc.*, 85 BNA's PTCJ 70**

The U.S. District Court for the Northern District of California on November 6, 2012 ruled that the developer of the popular Angry Birds video game failed to meet the heightened threshold of demonstrating in its trademark and copyright infringement lawsuit to win an *ex parte* temporary restraining order against alleged counterfeiters of Angry Birds merchandise.

***Temper-Pedic International Inc. v. Angel Beds LLC.*, 85 BNA's PTCJ 69**

The U.S. District Court for the Southern District of Texas on November 6, 2012 ruled that a complaint by the maker of Tempu-Pedic "memory foam" mattresses and pillows regarding a competitor's use of its trademarks in its website was sufficient to adequately notify the defendant of the claims and to allow it to craft an answer.

***Prosperity Bancshares Inc. v. Town and Country Financial Corp.*, 85 BNA's PTCJ 517**

The U.S. District Court for the Central District of Illinois on February 5, 2013 ruled that a Bank's locale in trademark dispute matters despite internet's potential to widen market.

***iCall Inc. v. Tribair Inc.*, 85 BNA's PTCJ 137**

The U.S. District Court for the Northern District of California on November 21, 2012 ruled that owner of iCall mark for VoIP services fails to enjoin competitor's use of WiCall mark.

***Jurin v. Google Inc.*, 104 USPQ2d 1480**

The U.S. District Court for the Eastern District of California on October 17, 2012 granted summary judgment to defendant internet search engine provider on Lanham Act and state-law claims based on defendant's use of plaintiff's "Styrotrim" mark as keyword that plaintiff's competitors may bid on to secure "sponsored link" that appears on search results page when users search for "Styrotrim," since plaintiff has proffered no evidence demonstrating that any likelihood-of-confusion factors weigh in his favor.

***Pair Networks Inc. v. Soon*, 85 BNA's PTCJ 521**

The U.S. District Court for the Western District of Pennsylvania on February 6, 2013 ruled that a cybersquatting infringer loses twitter handle by default.

***Timelines Inc. v. Facebook Inc.*, 85 BNA's PTCJ 823**

The U.S. District Court for the Northern District of Illinois on April 1, 2013 ruled that evidence that a social media company generically used the word "timeline" to drive traffic to its

website and discontinued the practice after such gains were optimized does not amount to a showing of such repeated use of the term that the company renders its registered "TimeLines" trademarks generic through its own actions.

Elcometer Inc. v. TQC-USDA Inc., 85 BNA's PTCJ 938

The U.S. District Court for the Eastern District of Michigan on April 9, 2013 ruled that a company whose authorized distributors allegedly bought a competitor's registered trademark as a Google adword could be held contributorily liable for federal and state trademark infringement.

Craigslist v. 3Taps, 86 BNA's PTCJ 7

The U.S. District Court for the Northern District of California on April 30, 2013 ruled that Craigslist's trademark infringement, breach of contract, and Computer Fraud and Abuse Act claims against services that allegedly scraped user-generated content from Craigslist's local classified ads and redistributed the data through their own proprietary systems survive dismissal.

J.T. Colby & Co. d/b/a Brick Tower Press v. Apple, 86 BNA's PTCJ 135

The U.S. District Court for the Southern District of New York on May 8, 2013 ruled that a group of publishing companies asserting unregistered trademark rights in the term "ibooks" against Apple Inc. fails to establish that it had any enforceable trademark rights or that Apple's use of "iBooks" for its e-reader software would create a likelihood of reverse confusion.

General Steel Domestic Sales v. Chumley, 86 BNA's PTCJ 188

The U.S. District Court for the District of Colorado on May 7, 2013 ruled that Armstrong Steel Corp.'s use of a competitor's trademarked term as a keyword in its Google AdWords campaign does not constitute trademark infringement because it was not likely to confuse consumers.

Deckers Outdoor Corp. v. Does 1-100, 105 USPQ2d 1899

The U.S. District Court for the Northern District of Illinois on January 16, 2013 granted a preliminary injunction to plaintiff alleging infringement of its "UGG" trademarks for footwear against defendant anonymous entities selling counterfeit products on internet; pursuant to TRO already in effect, defendants' "PayPal" and other accounts associated with accused internet domain names will remain frozen.

Kerodin v. ServiceMagic Inc., 106 USPQ2d 1425

The U.S. District Court for the District of Maryland on March 11, 2013 ruled that plaintiffs have failed to allege facts demonstrating that they hold exclusive ownership of nine domain names at issue, since plaintiffs' registration of domain names in 2006 was not sufficient, by itself, to establish ownership over alleged marks, and plaintiffs have not alleged that they engaged in continuous commercial use of marks during months and years preceding initiation of instant action in 2011.

True Fit Corp. v. True & Co., 106 USPQ2d 1405

The U.S. District Court for the District of Massachusetts on March 4, 2013 ruled that infringement plaintiff is not likely to succeed on merits of claim that defendant e-commerce lingerie retailer's use of term "True" infringes plaintiff's "Find Your True Fit," "True Fit," and "True to You" trademarks, and preliminary injunction that would prohibit defendant from using marks containing word "True" in connection with personalized fit-matching software and services is denied.

Macy's Inc. v. Strategic Marks LLC, 106 USPQ2d 1582

The U.S. District Court for the Northern District of California on March 19, 2013 denied summary judgment to plaintiffs that defendant has not satisfied Lanham Act's use-in-commerce requirement for service marks that are subject of defendant's infringement counterclaim, even though defendant has created website that describes its proposed retail business, but has not sold accessories, apparel, or other products, and has not opened boutiques or stores referenced on its site, since defendant owns federal registrations for marks, and there are disputed issues of material fact as to whether defendant's sales- and nonsales-related activities suffice to meet use-in-commerce requirement.

Dudley d/b/a HealthSource Chiropractic v. HealthSource Chiropractic Inc., 84 BNA's PTCJ 669

The U.S. District Court for the Western District of New York on August 7, 2012 ruled that the internet is not geographic zone over which one mark holder can have exclusive rights.

Amerigas Propane LP v. Opinion Corp. d/b/a Pissedconsumer.com, 84 BNA's PTCJ 418

The U.S. District Court for the Eastern District of Pennsylvania on June 19, 2012 accepted a claim of initial interest confusion in case against online gripe site.

***Montblanc-Simplo GmbH v. Cheapmontblancpens.com*, 101 USPQ2d 1161**

The U.S. District Court for the Eastern District of Virginia on July 5, 2012 ruled that plaintiff asserting in rem action for violation of Anticybersquatting Consumer Protection Act against 265 internet domain names is granted default judgment on its claim for relief under 15 U.S.C. § 1125(D)(1), since accused domain names are confusingly similar to plaintiff's "Montblanc" mark, and since registrants of domain names have demonstrated bad-faith intent to profit from plaintiff's mark; permanent injunction orders transfer of infringing domain names to plaintiff.

***Libya v. Miski*, 103 USPQ2d 1927**

The U.S. District Court for the District of Columbia on September 6, 2012 ruled that plaintiff's "Embassy of Libya" and "Libyan Embassy" marks are descriptive, and absent evidence of secondary meaning, plaintiffs cannot pursue trademark infringement and anticybersquatting claims against "expeditor of document legalization for use of domain names such as "embassyoflibya.org".

***Florida VirtualSchool v. K12 Inc.*, 103 USPQ2d 1853**

The U.S. District Court for the Middle District of Florida on July 16, 2012 ruled that Florida law that converted plaintiff provider of online educational courses into state agency, Fla. Stat. § 1002.37, does not grant plaintiff ownership of "Florida VirtualSchool" and "FLVS" trademarks that plaintiff used and registered with U.S. Patent and Trademark Office, since statute permits plaintiff's board of trustees to "acquire, enjoy, use and dispose of patents, copyrights, trademarks, licenses, and rights or interests thereunder or therein," but states that "[o]wnership of all such" intellectual property "shall vest in the state, with the board having full right of use and full right to retain the revenues derived therefrom."

TRADEMARKS – *Case Law* – U.S. Patent and Trademark Office

***In re Azteca Systems Inc.*, 102 USPQ2d 1955**

The Trademark Trial and Appeal Board on April 19, 2012 ruled that Applicant's "GIS Empowered by Cityworks" mark, as displayed on webpage submitted by applicant as specimen of use, fails to create association with applicant's computer software for management of public works and utilities assets, and fails to serve as indicator of source of those goods, since mark is distant from description of software on webpage, and is separated from that description by more than 15 lines of text concerning marginally related topics.

***City National Bank v. OPGI Management GP Inc./Gestin OPGI Inc.*, 106 USPQ2d 1668**

The Trademark Trial and Appeal Board on April 26, 2013 ruled that respondent management company, in cancellation proceeding, has failed to demonstrate that it has ever used disputed term "TreasuryNet" as mark in commerce in connection with recited services of providing financial information, since respondent claims that it provides financial information directly to its employees through "TreasuryNet" database on its intranet site, but primary beneficiary of such services is respondent itself, not employees who are accessing database in order to perform their jobs.

***Embarcadero Technologies Inc. v. RStudio Inc.*, 105 USPQ2d 1825**

The Trademark Trial and Appeal Board on February 14, 2013 ruled that applicant facing claim of likelihood of confusion in opposition proceeding has established successful defense, under 15 U.S.C. § 1068, based on amended description of goods and services in its applications for registration of "RStudio" mark for software and related services.

***America's Best Franchising Inc. v. Abbott*, 106 USPQ2d 1546**

The Trademark Trial and Appeal Board on March 20, 2013 ruled that fact that parties' marketing efforts for their respective "3 Palms" hotels "overlap" on internet does not mean that relevant territory, for purposes of concurrent use proceeding, is entire United States, since hotel services are by definition rendered in particular geographic location, even if they are also offered, by same ultimate source, in other locations under same mark, since creation of internet has not rendered Lanham Act's concurrent-use provisions moot, and since fact that both parties' services are promoted and offered online is not sufficient to result in likelihood of confusion.

***In re Rogowski*, 85 BNA's PTCJ 287**

The Trademark Trial and Appeal Board on December 11, 2012 ruled that a YouTube screen shot of a trademark does not show "use in commerce" for registration purposes.

***In re Powermat*, 85 BNA's PTCJ 415**

The Trademark Trial and Appeal Board on January 17,

2013 ruled that a sequence of "chirp" sounds that play when a cell phone is placed on or taken off a battery charging device is not inherently distinctive, and thus the sound mark is not eligible for registration. The board notes that the battery chargers in fact emit chirp sounds in their normal course of operation.

***ChaCha Search Inc. v. Grape Technology Group Inc,* 105 USPQ2d 1298**

The Trademark Trial and Appeal Board on December 27, 2012 granted summary judgment to opposer that its involved service mark "242242" is not merely descriptive of its search engine services for obtaining specific user-requested information, even though mark identifies short message services (i.e. SMS) number, used to send messages between mobile telephones, through which customers obtain opposer's services, since SMS number does not identify ingredient, quality, characteristic, function, feature, purpose, or use of opposer's services simply because it provides means of accessing those services.

TRADEMARKS – *Case Law* – State Court – California

***Tre Miklano LLC v. Amazon.com Inc.,* 84 BNA's PTCJ 758**

The California Court of Appeal, Second District, on August 22, 2012 ruled that notice of alleged infringement creates no duty for Amazon to remove listing.

TRADEMARKS – *Case Law* – State Court – Massachusetts

***Jenzabar Inc. v. Long Bow Group Inc.,* 85 BJA's PTCJ 14**

The Massachusetts Appeals Court on October 18, 2012 ruled that a film producer's use of a former Tiananmen Square protestor's trademarks in metatags on its Tiananmen Square documentary's website was not infringing.

TRADEMARK/CYBERSQUATTING – *Case Law* – U.S. Court of Appeals

***Pensacola Motor Sales Inc. v. Eastern Shore Toyota LLC,* 84 BNA"s PTCJ 423**

The U.S. Court of Appeals for the Eleventh Circuit on June 21, 2012 ruled that jury instruction error did not bolster mark owner's ACPA appeal.

TRADEMARK/CYBERSQUATTING – *Case Law* – U.S. District Court

***Aviva USA Corp. v. Vazirani,* 84 BNA"s PTCJ 1035**

The U.S. District Court for the District of Arizona on October 2, 2012 ruled that "Cybergripe" site did not make commercial use of plaintiff's trademarks, trade dress.

***Louis Vuitton Malletier S.A. v. 100Wholesale.com,* 85 BNA's PTCJ 290**

The U.S. District Court for the Southern District of Florida on November 30, 2012 issued a preliminary injunction compelling disclosures from proxies in a mass cybersquatting case.

***ViaView Inc. v. Blue Mist Media,* 105 USPQ2d 1304**

The U.S. District Court for the District of Nevada on November 30, 2012 ruled that plaintiff claiming rights in term "isanyoneup" as trademark for its campaign to stop "bullying behavior" is likely to succeed on merits of claim that defendants' use of term "isanyoneup," in domain names for websites where they publish "involuntary pornography," violates Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d), and plaintiff is granted temporary restraining order prohibiting defendants from using term in domain names for their sites.

TRADEMARKS/RIGHT OF PUBLICITY – *Case Law* – U.S. District Court

***Fraley v. Facebook Inc.,* 104 USPQ2d 1630**

The U.S. District Court for the Northern District of California on August 17, 2012 denied preliminary approval to parties' agreement to settle class action, alleging violations of California law stemming from use of names and/or likenesses of members of defendant social networking website to promote products and services through "Sponsored Stories" advertising practice, since provisions awarding $10 million cy pres payment to organizations involved in internet privacy issues, and permitting plaintiffs to apply for up to $10 million in attorneys' fees without objection by defendant, raise serious concerns.

TRADEMARKS/UNFAIR COMPETITION – *Case Law* – U.S. District Court

***Allure Jewelers Inc. v. Ulu,* 104 USPQ2d 1231**

The U.S. District Court for the Southern District of Ohio on September 20, 2012 ruled that plaintiff has failed to state claim for "hot news" misappropriation under common law by

alleging that defendant improperly "scraped" or copied information about jewelry and gold items from plaintiff's internet advertisements for use in defendant's advertisements for same products, since, even if it is assumed that "hot news" misappropriation claim would survive preemption by federal copyright law, there is no support for such claim under Ohio law.

TRADEMARKS/UNFAIR TRADE PRACTICES – *Case Law* – U.S. Court of Appeals

***Contour Design Inc. v. Chance Mold Steel Co.,* 104 USPQ2d 1509**

The U.S. Court of Appeals for the First Circuit on September 4, 2012 ruled that defendant's computer mouse was not "derived from" plaintiff's design in violation of parties nondisclosure agreement; "derivation" requires appropriation of some novel property of plaintiff's products.

TRADE SECRETS – *Case Law* – U.S. Court of Appeals

***United States v. Howley,* 85 BNA's PTCJ 472**

The U.S. Court of Appeals for the Sixth Circuit on February 4, 2013 ruled that evidence that two engineers secretly took pictures of some of Goodyear's equipment – which the company that employed the engineers is trying to recreate – is sufficient to sustain the engineers' criminal convictions under the Economic Espionage Act of 1996, 18 U.S.C. § 1832. The defendants, who were visiting Goodyear's plant in order to do repair work on some machines, took the photographs using a cell phone and did so only after they had been left alone by Goodyear employees.

***MacDermid Inc. v. Deiter,* 105 USPQ2d 1500**

The U.S. Court of Appeals for the Second Circuit on December 26, 2012 ruled that Connecticut's long-arm statute permits exercise of jurisdiction over former employee of plaintiff who sent, via e-mail, plaintiff's allegedly confidential and proprietary information from her business account to her personal account, even though defendant physically interacted only with computers in Canada when sending e-mail at issue.

***Wellogix Inc. v. Accenture LLP,* 106 USPQ2d 1796**

The U.S. Court of Appeals for the Fifth Circuit on May 15, 2013 ruled that once plaintiff makes out *prima facie* case for existence of trade secret, burden is on defendant to show that patent covers same subject matter, and therefore discloses, claimed trade secret; in present case, in which plaintiff's patents were not introduced into record, plaintiff presented sufficient evidence to support jury's finding that plaintiff's software for estimating well construction costs in oil and gas industry contained trade secrets.

TRADE SECRETS – *Case Law* – U.S. District Court

***Wang v. Palo Alto Networks Inc.,* 85 BNA's PTCJ 483**

The U.S. District Court for the Northern District of California on January 31, 2013 ruled that a U.S. patent application on firewall technology contained trade secrets at least until the patent application was published.

***Beacon Wireless Solutions Inc. v. Garmin International, Inc.,* 103 USPQ2d 1721**

The U.S. District Court for the Western District of Virginia on May 9, 2012 denied summary judgment that plaintiffs lack trade secret protection for combination of design features for their vehicle fleet management system, and in technical information provided to defendants in development of software application; however, defendants are granted summary judgment that they did not misappropriate trade secrets embodied in plaintiffs' source code and other technical details of their software.

***Ameriprise Financial Services Inc. v. Koenig,* 104 USPQ2d 1280**

The U.S. District Court for the District of New Jersey on February 6, 2012 ruled that plaintiff financial services firm has shown likelihood of success on merits of its claim for breach of employment agreement against defendant former employee, who sent protected client information to his personal e-mail address before leaving firm to work for competitor; however, plaintiff has not established likelihood of success on merits of its claim for misappropriation of trade secrets, since information defendant forwarded likely contained trade secrets, but extent of resulting harm is unclear.

***Beacon Wireless Solutions Inc. v. Garmin International, Inc.,* 103 USPQ2d 1721**

The U.S. District Court for the Western District of Virginia on May 9, 2012 denied summary judgment that plaintiffs lack trade secret protection for combination of design features for their vehicle fleet management system, and in technical information provided to defendants in development of software application; however, defendants are granted summary judgment that they did not misappropriate trade secrets embodied in plaintiffs' source code and other technical details of their software.

TRADE SECRETS/CRIMINAL – *Case Law* – U.S. District Court

***United States v. Yang*, 84 BNA's PTCJ 920**

The Justice Department in the U.S. District Court for the Northern District of Illinois on September 19, 2012 announced that Chunlai Yang, an ex-software engineer at CME Group Inc. pled guilty to two counts of trade secret theft based on his illicit downloading of CME trade secrets and source code relating to CME's "Globex" trading platform, which he intended to use to develop a trading platform for the Zhangjiagang China chemical electronic trading exchange. Yang now faces a maximum of 10 years in prison and a $250,000 fine for each count.

TRADE SECRETS/CRIMINAL – *Case Law* – State Court - New York

***People v. Aleynikov*, 84 BNA's PTCJ 675**

The District Attorney for New York County Criminal Court on August 9, 2012 announced that a former programmer at Goldman Sachs faces state charges over code theft.

COMPUTER FRAUD AND ABUSE ACT (CFAA) – *Case Law* – U.S. Court of Appeals

***United States v. Nosal*, 676 F.3d 854**

The U.S. Court of Appeals for the Ninth Circuit on April 10, 2012 in an *en banc* decision, adopted a narrow reading of the Computer Fraud and Abuse Act, finding that violating an employer computer policy or a website's terms of service is not a violation of federal law.

***WEC California Energy Solutions LLC v. Miller*, 687 F.3d 199**

The U.S. Court of Appeals for the Fourth Circuit on July 26, 2012 sided with the Ninth Circuit in deciding that the Computer Fraud and Abuse Act does not apply to employees and former employees who were authorized to access the employer's electronic information. The decision stands in contrast to the position taken by the Seventh Circuit in *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). The Fourth Circuit rejects the interpretation of the CFAA taken by the Seventh Circuit, which interprets the CFAA much more broadly. The Seventh Circuit concludes that an employee's misappropriation of electronic information from his employer is a breach of the employee's duty of loyalty that immediately terminates his agency relationship and with it his authority to access the laptop, because the only basis of his authority had been that relationship.

LANHAM ACT – *Case Law* - U.S. District Court

***Invent Worldwide Consulting LLC v. Absolutely News Inc.*, 84 BNA's PTCJ 919**

The U.S. District Court for the Northern District of Illinois on September 19, 2012 ruled that Web posts calling competitor testimonials "scam" could generate Lanham Act liability.

***Apple v. Amazon.com*, 85 BNA's PTCJ 349**

The U.S. District Court for the Northern District of California on January 2, 2013 ruled that Apple Inc. cannot proceed with a false advertising claim targeting Amazon's use of the name "appstore".

***M-Edge Accessories v. Amazon.com*, 85 BNA's PTCJ 386**

The U.S. District Court for the District of Maryland on January 2, 2013 ruled that Amazon's designation of a rival Kindle accessories maker's products as "unavailable" may generate false advertising liability under the Lanham Act.

RIGHT OF PUBLICITY – *Case Law* - U.S. Court of Appeals

***Hart v. Electronic Arts*, 86 BNA's PTCJ 183**

The U.S. Court of Appeals for the Third Circuit on May 21, 2013 held that a video game maker's "realistic representation[]" of a Rutgers University quarterback is not transformative, and therefore the use of the player's likeness is not protectable expression under the First Amendment.

PRIVACY – *Case Law* – State Court – Wisconsin

***Habush v. Cannon*, 85 BNA's PTCJ 570**

A Wisconsin state appeals court on February 21, 2013 ruled that a law firm that purchased the names of rival law firm partners as invisible search advertising keywords did not "use" the individuals' names in violation of Wisconsin's invasion of privacy statute.

PRIVACY – *State Legislation* – Michigan

Governor Snyder on December 27, 2012 signed H.B. 5523 into law as Public Act 478 which prohibits requesting or requiring an employee, student or applicant to disclose a user name or password for a personal social media account. The law applies to employers and academic institutions.

FOREIGN CASE/COURT – *Case Law* – Europe/European Union

***UsedSoft GmbH v. Oracle International Corp.*, 84 BNAs PTCJ 433**

The European Court of Justice on July 3, 2012, ruled that Oracle software buyers may resell "used" downloaded copies under first sale doctrine.

FOREIGN CASE/COURT – *Case Law* – France

***Auto IES v. Google France*, 84 BNA's PTCJ 1009**

A chamber of the Supreme Court of France on September 25, 2012 ruled that Google AdWords advertisers do not necessarily infringe marks.

FOREIGN CASE/COURT – *Case Law* – United Kingdom

***Public Relations Consultants Association Limited v. Newspaper Licensing Agency Limited*, 85 BNA's PTCJ 915**

The UK Supreme Court on April 17, 2013 recognizing the transnational dimension and important implications of the matter for internet users, referred to the European Court of Justice a case exploring the copyright implications of viewing copyrighted material on a computer screen. ▪