State Bar of Michigan

Michigan IT Lawyer

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

http://www.michbar.org/computer

Table of Contents

March 2011 ▪ Vol. 28, Issue 2

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/computer/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 Chair

By Mark G. Malven, *Dykema Gossett PLLC*

I hope all of you are enjoying our beautiful Spring weather here in Michigan. (NOTE: I write this knowing that by the time this is published it may well be snowing again!) As your Chair I wanted to let you know about some recent and upcoming events.

On the evening of March 10, in conjunction with our Council Meeting, we sponsored a presentation by Professor John Rothchild at Wayne State University Law School on the currently hot topic of "Net Neutrality" and the related legislative and regulatory efforts by the FCC. Thank you, Professor Rothchild, for a very informative and entertaining presentation. Also, a special thank you to Council member Nilay Davé for his suggestion of Prof. Rothchild, and for his hard work arranging this event.

We also have a number of valuable activities upcoming:

- On **Thursday April 21**, we will be co-sponsoring a **Spring Networking Event** at **The Post Bar in Novi from 5 to 8 pm**. This will be a reprise of our successful spring networking event last year in conjunction with DetroitNET.org, which is one of the largest networking groups for IT professionals in the region. Last year was great fun and this will be a can't-miss event.

- We will be sponsoring an **IT Law-themed edition** of the **July *Michigan Bar Journal***.

- Our **Fourth Annual Information Technology Law Seminar** will be **Wednesday, September 21, 2011**. Based on the success of the 2010 seminar, the seminar will once again be presented as an all-day format, from 9 a.m. to 4 p.m., with a cocktail reception afterward. We are again working in cooperation with the Institute for Continuing Legal Education (ICLE), and the venue is the St. John's Inn in Plymouth, with

Continued on next page

a webcast also available. There are **sponsorship spots still available**, so if your organization would be interested please contact Charlie Bieneman at cab@raderfishman.com.

- Our **Annual Meeting** will be **Wednesday, September 21, 2011** during the lunch session of the IT Law ICLE Seminar. If you have any questions, please feel free to contact me at mmalven@dykema.com.

If you have any suggestions, comments etc. for how we may be of further service to you as a member of the IT Law Section, please do not hesitate to contact me.

Best regards, Mark Malven

Save the Date!!!

On **Thursday, April 11, 2011**, instead of doing something taxing, plan on something more relaxing: Join the *Information Technology Law Section* for our ***Spring Networking Event***! This year we are again joining forces with *DetroitNET.org* at *The Post Bar*, 42875 Grand River Avenue, Novi, Michigan, from 5 to 8 PM. Our Section will be a co-sponsor of one of Michigan's premier I.T. networking events, which is attended by hundreds of I.T. professionals, recruiters, job-seekers and lawyers. And best of all, the event is FREE to attend! Registration details will be available soon. For more information, check *www.detroitnet.org*!

The Fourth Annual Information Technology Law Seminar will be **Wednesday, September 21, 2011**, from 9 a.m. to 4 p.m. Reserve the date on your calendar, and plan to take advantage of a great line up of speakers while receiving continuing legal education credit! Based on the success of the 2010 seminar, the conference will once again be presented as an all-day format. Once again the Information Technology Law Section of the State Bar of Michigan is working in cooperation with the Institute for Continuing Legal Education (ICLE), and the venue is the St. John's Inn in Plymouth, with a webcast also available. If you know of an organization that may be interested in sponsoring the event, please contact *Charlie Bieneman* at *cab@raderfishman.com*. Watch for further details over the upcoming months, and please save the date!

Attend the Information Technology Section's ***Annual Business Meeting***. Mingle with Section peers, learn about opportunities to get more involved with the Section, and participate in the election of Section Council Members. The Information Technology Section's 2011 Business Meeting will be held during the lunch session of the Fourth Annual Information Technology Law Seminar. Be there! Please contact *Mark Malven* at MMalven@dykema.com if you have questions about the event. ■

Recent Developments in Information Technology Law

By David R. Syrowik, *Brooks Kushman P.C.*

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

As reported at 81 BNA's PTCJ 137, on November 29, 2010 the U.S. Supreme Court, in a case involving the popular Word program, grants a petition for writ of certiorari in Microsoft Corp.'s attack on the clear-and-convincing evidence standard for challenges to the validity of a patent. Lowering the standard to a preponderance of evidence – as Microsoft requests – could significantly decrease the strength of every patent owner's case in litigation. *Microsoft Corp. v. i4i L.P.*

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

As reported at 81 BNA's PTCJ 140, on November 29, 2010 the U.S. Supreme Court, declines review of a case in which a defendant accused of infringing copyrights in sound recordings by making unauthorized copies through online downloading is denied the opportunity to pursue an innocent infringer defense. *Harper v. Maverick*.

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

As reported at 81 BNA's PTCJ 141, on November 29, 2010 the U.S. Supreme Court denies a petition for a writ of certiorari in a case appealing the Second Circuit's ruling that online auction site operator eBay Inc. is not liable for trademark infringement or dilution – either directly or secondarily – based on some sellers' listing of counterfeit Tiffany jewelry, because it takes action when it has knowledge of fraud with regard to any specific listing. *Tiffany (NJ) Inc. v. eBay Inc.*

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

As reported at 81 BNA's PTCJ 315 on January 10, 2011 the U.S. Supreme Court lets stand a Second Circuit decision allowing antitrust allegations to proceed against four of the nation's major music labels. Consequently, the music labels' internet pricing collusion case will go forward. *Sony Music Entertainment v. Starr.*

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

As reported at 81 BNA's PTCJ 55, on November 4, 2010 the U.S. Court of Appeals of the Federal Circuit ruled that computer system and storage medium claims in a software patent were infringed but method claims were not infringed by competitors' computer security products. *Finjan Inc. v. Secure Computing Corp.*

As reported at 81 BNA's PTCJ 342, on January 11, 2011 the U.S. Court of Appeals for the Federal Circuit ruled that a patent owner's lawsuit against Google Inc. was not "objectively baseless," reversing a lower court's award of $626,000 in attorneys' fees to Google as sanctions for the patent owner's frivolous claims. *iLOR LLC v. Google Inc*.

As reported at 81 BNA's PTCJ 171, on December 8, 2010 the U.S. Court of Appeals for the Federal Court held, in delivering its first ruling on patentable subject matter since the U.S. Supreme Court's *Bilski v. Kappos* decision, that to be found unpatentable under 35 U.S.C. § 101, an invention's abstractness must "exhibit itself so manifestly as to override the broad statutory categories" of patent eligibility. *Research Corporation Technologies Inc. v. Microsoft Corp.*

As reported at 81 BNA's PTCJ 173, on December 7, 2010 the U.S. Court of Appeals for the Federal Circuit ruled that a patent on an invention that simply replaced a phone-and-fax based solution with an internet-based approach was invalid for obviousness. The court reverses the district court's award of $16.5 million for infringement of Western Union Co.'s patents on money transfers using the internet to set up the transactions. *Western Union Co. v. MoneyGram Payment Systems Inc.*

As reported at 81 BNA's PTCJ 371, on January 20, 2011 the U.S. Court of Appeals for the Federal Circuit ruled that an infringing "use" of a system patent claim occurs if one party within the system performs an action putting the rest of the system into service. The court holds that an infringing use of a multi-device computing system by an end user does not require physical control over all the devices. *Centillion Data Systems LLC v. Qwest Communications International Inc.*

As reported at 81 BNA's PTCJ 275, on January 4, 2011 the U.S. Court of Appeals for the Federal Circuit overturned a district court's award of judgment as a matter of law that Microsoft Corp. was not liable for infringement of a patent on software copying protection. A $388 million jury award is vacated, but Microsoft will now have to face the jury again on the damages issue alone. *Uniloc USA v. Microsoft Corp.*

PATENT/PERSONAL JURISDICTION/VENUE – *Case Law* – U.S. Courts of Appeal

As reported at 97 USPQ 2d 1351, on November 12, 2010 the U.S. Court of Appeals for the Federal Circuit ruled that foreign infringement defendant purposely directed its activities at residents of forum state, since defendant imported allegedly infringing software into California, entering into agreement with California company to provide assistance in selling accused products, and received more than 95 percent of profits from sale of software. *Nuance Communications Inc. v. Abbyy Software House*.

As reported at 81 BNA's PTCJ 308, on January 5, 2011 the U.S. Court of Appeals for the Federal Circuit transfers a case out of the eastern district of Texas, rejecting a patent owner's attempt to manipulate the venue choice by incorporating an affiliate office in Tyler, Texas, without employees. *In re Microsoft Corp.*

COPYRIGHTS/PERSONAL JURISDICTION – *Case Law* – U.S. Courts of Appeal

As reported at 96 USPQ 2d 1349, on August 5, 2010 the U.S. Court of Appeals for the Second Circuit held that defendant California resident's contacts with New York are sufficient to subject him to personal jurisdiction under state's "single-act" long-arm statute, since defendant shipped counterfeit "Chloé" handbag to purchaser in New York, and since defendant's company operated interactive website offering handbags for sale to New York consumers, and shipped merchandise to New York on 52 other occasions. *Chloé* v. *Queen Bee of Beverly Hills LLC*.

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

As reported at 81 BNA's PTCJ 309, on January 4, 2011 the U.S. Court of Appeals for the Ninth Circuit ruled that the distribution of promotional copies of music CDs by a record company resulted in transfer of title of those CDs, and thus sale of those discs at online auctions was protected under the first sale doctrine. *UMG Recordings Inc. v. Augusto*.

As reported at 81 BNA's PTCJ 373, on January 19, 2011 the U.S. Court of Appeals for the Seventh Circuit ruled that a licensee of insurance software did not hold any of the exclusive rights enumerated under the Copyright Act and thus did not have standing to bring an infringement claim against another licensee that had allegedly exceeded the scope of its license. *Hyperquest Inc. v. N'Site Solutions*.

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

As reported at 81 BNA's PTCJ 251, on December 14, 2010 the U.S. Court of Appeals for the Ninth Circuit held that Congress, in enacting the Digital Millennium Copyright Act in 17 U.S.C. § 1201(a)(2), gave digital content owners a new legal protection against technologies that circumvent access controls protecting their digital property. *MDY Industries LLC v. Blizzard Entertainment Inc.*

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

As reported at 81 BNA's PTCJ 19, on October 27, 2010 the U.S. Court of Appeals for the Ninth Circuit ruled that using a domain name with bad faith intent by holding it for ransom gives rise to liability under the Anti-cybersquatting Consumer Protection Act. *DSPT International Inc. v. Nahum*.

As reported at 81 BNA's PTCJ 281, on December 20, 2010 the U.S. Court of Appeals for the Seventh Circuit ruled that in determining whether the use of two registered trademarks would be likely to create an assumption in the minds of consumers that the software products came from the same source, a district court erred in limiting its analysis to the description of the goods as found in the respective trademark registrations. *Board of Regents of the University of Wisconsin System v. Phoenix Software International Inc.*

As reported at 81 BNA's PTCJ 526, on February 16, 2011 the U.S. Court of Appeals for the Ninth Circuit ruled that a cybersquatter who succeeded in getting a trademark infringement judgment vacated 15 months earlier loses his second appeal, in that the lower court properly followed instructions on differentiating suggestive versus descriptive marks. *Lahoti v. Vericheck Inc.*

TRADEMARKS/PERSONAL JURISDICTION – *Case Law* – U.S. Courts of Appeal

As reported at 96 USPQ 2d 1921, on October 1, 2010 the U.S. Court of Appeals for the Seventh Circuit ruled that defendant Texas-based professional association, which provides on-site anesthesiology services, does not have minimum contacts with Illinois sufficient to justify exercise of specific personal jurisdiction by Illinois federal court in cybersquatting action; defendant's operation of website accessible to Illinois residents, with domain name similar to plaintiff's "Mobile Anesthesiologists" mark, does not constitute action "expressly aimed" at forum state with intent to harm. *Mobile Anesthesiologists Chicago LLC v. Anesthesia Associates of Houston Metroplex PA*.

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

As reported at 81 BNA's PTCJ 297, on December 28, 2010 Interval, a Seattle-based patent licensing firm formed by Microsoft's co-founder, Paul Allen, amends suit in the U.S. District Court for the Western District of Washington for internet giants' (including Apple, AOL, eBay, Facebook, Google, Netflix, YouTube) patent infringement. *Interval Licensing LLC v. AOL Inc.*

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

As reported at 80 BNA's PTCJ 842, on October 19, 2010 the U.S. District Court for the District of Nevada ruled that real estate company's blog posting of a newspaper article did not infringe the copyright held by Righthaven LLC, which is engaged in lawsuits challenging the internet posting and aggregation of newspaper content. *Righthaven LLC v. Realty One Group Inc.*

As reported at 81 BNA's PTCJ 426, on January 14, 2011 the U.S. District Court for the Southern District of New York ruled that Twitter's terms of service, which granted Twitter and affiliated websites a license to use and reproduce uploaded photographs, does not clearly confer a right on other users to reuse copyrighted postings. *Agence France-Presse v. Morel.*

As reported at 80 BNA's PTCJ 54, on November 4, 2010 a jury in the U.S. District Court for the District of Minnesota concluded that Jammie Thomas-Rasset, the first peer-to-peer file sharer to defend infringement litigation all the way to a verdict, should pay $1.5 million in statutory damages for willfully sharing 24 copyrighted music files. *Capitol Records Inc. v. Thomas-Rasset*.

As reported at 97 USPQ 2d 1667, on December 28, 2010 the U.S. District Court for the Northern District of California ruled that plaintiff motion picture production company, which claims that anonymous defendants used online peer-to-peer network to reproduce plaintiff's copyrighted movie, has shown good cause for permitting it to engage in early discovery in order to identify anonymous defendants and effect service of process. *Patrick Collins Inc. v. Does 1-1219*.

As reported at 81 BNA's PTCJ 57, on October 28, 2010 the U.S. District Court for the District of Nevada ruled that operators of a Canadian website, on which an anonymous user posted a copyrighted news article, must defend the case in Nevada. *Righthaven LLC v. Major-Wager.com Inc.*

As reported at 81 BNA's PTCJ 88, on November 9, 2010 the U.S. District Court for the Southern District of New York ruled that a software developer may be a joint author of a former partner's enhancements. *Exceller Software Corp. v. Pearson Education Inc.*

As reported at 81 BNA's PTCJ 89, on November 3, 2010 the U.S. District Court for the Southern District of California approved expedited discovery on ISPs in a lawsuit arising from walled website misuse. *Liberty Media Holdings, LLC v. Does 1-59*.

As reported at 81 BNA's PTCJ 109, on November 27, 2010 the U.S. District Court for the Southern District of New York ruled that Gawker.com's online publication of 21 pages from Sarah Palin's *America By Heart*, days before the book's release, was likely infringing and not fair use. *Harper Collins Publishers LLC v. Gawker Media LLC*.

As reported at 81 BNA's PTCJ 114, on November 17, 2010 the U.S. District Court of the Northern District of California ruled that dancing kids YouTube poster's email was not protected by attorney-client privilege. Magistrate judge did not clearly err in granting defendant copyright owners' motion to compel further discovery with respect to plaintiff's communications with her attorneys regarding her motives for bringing lawsuit against defendants for alleged misrepresentations in "takedown" notice, issued under 17 U.S.C. § 512(c)(3), which warned against potential infringement and instructed video hosting site to remove plaintiff's home video. *Lenz v. Universal Music Corp.*

As reported at 97 USPQ 2d 1664, on December 21, 2010 the U.S. District Court for the Northern District of California ruled that plaintiff has raised serious questions going to merits of its Digital Millennium Copyright Act claim alleging that defendant, in DMCA "takedown" notice, materially misrepresented that plaintiff's virtual horse products infringe defendant's copyrights in virtual rabbits, since defendant cannot prevent plaintiff from marketing virtual animals with similar traits, provided defendant's programming was not copied and since plaintiff submitted declarations to that effect. *Amaretto Ranch Breedables v. Ozimals Inc.*

As reported at 81 BNA's PTCJ 145, on November 22, 2010 the U.S. District Court for the District of Columbia as asked by the plaintiff in a copyright infringement action against thousands of users of BitTorrent to sanction a Florida defense attorney who has sold "do-it-yourself" packages to some of the defendants. *Voltage Pictures LLC v. Doe*.

As reported at 97 USPQ 2d 1178 on March 19, 2010 the U.S. District Court for the Northern District of California ruled that digital image data stored on computer may constitute "copy" under Copyright Act, since image is "fixed in a tangible medium of expression," for purposes of Copyright Act, when it is stored on computer's server, hard disk, or other

storage device, and since computer owner shows copy by means of device or process when owner uses computer to fill computer screen with image stored on that computer, or communicates stored image electronically to another computer. *Louis Vuitton Malletier SA v. Akanoc Solutions Inc.*

As reported at 96 USPQ 2d 1787, on September 1, 2010 the U.S. District Court for the Northern District of California dismissed a counterclaim alleging infringement of copyright in computer software without leave to amend, since counterclaim pleads facts showing that software at issue is different from software described in defendant's registration certificate and supplementary registration, and since defendant's allegations regarding which version of software was deposited with the U.S. Copyright Office are ambiguous and inconsistent. *KEMA Inc. v. Koperwhats*.

As reported at 96 USPQ 2d 1934, on August 4, 2010 the U.S. District Court for the Eastern District of Virginia held that plaintiff's claim for conversion, based on defendant's use of plaintiff's manuscripts in plagiarism detection service database, is preempted by federal copyright law, since works at issue fall within subject matter of copyright protection, since claim seeks to hold defendant liable for encroaching on plaintiff's right to use and reproduce copyrighted work, and since plaintiff does not allege that defendant is retaining physical object that belongs to plaintiff, or claim that she owns digital code in which her work is stored on defendant's system. *Christen v. iParadigms LLC*.

As reported at 81 BNA's PTCJ 432, on January 19, 2011 the U.S. District Court for the Northern District of California dismissed a misuse counterclaim that *Adobe* had violated the first sale doctrine in a software infringement case. *Adobe Systems Inc. v. Kornrumph.*

As reported at 81 BNA's PTCJ 520, on February 22, 2011 the U.S. District Court for the Southern District of New York enjoined the service of a company that takes broadcast television signals off the air and streams them to subscribers over the internet by stating that the company is not a cable television service provider that is eligible for a statutory license granted to cable services under federal copyright law. *WPIX Inc. v. ivi Inc.*

As reported at 81 BNA's PTCJ 468, on February 3, 2011, the U.S. District Court for the Northern District of California ruled that neither the use of the same internet service provider and the same peer-to-peer network, nor the possibility of potential conspirator liability, can form the basis for a joinder of 435 Doe defendants that did not directly exchange copyrighted works with each other. *IO Group Inc. v. Doe*.

As reported at 81 BNA's PTCJ 469, on February 2, 2011 in the U.S. District Court for the Southern District of New York, federal prosecutors and custom authorities announced that domains were seized for publishing hyperlinks to unauthorized sports video streaming. *United States v. HQ-Streams.com*.

As reported at 97 USPQ 2d 1583, on January 11, 2011 the U.S. District Court for the Northern District of California ruled that it takes jurisdiction over claim alleging that defendant infringed copyright in musical composition by creating video set to copyrighted song and posting it on web, since Copyright Act does not apply to conduct that occurs abroad, and creation of accused video occurred entirely in Canada. *Shropshire v. Canning*.

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

As reported at 81 BNA's PTCJ 90, on October 21, 2010 the U.S. District Court for the Eastern District of California ruled that infringement notices to eBay involving furniture design likely violated DMCA. *Design Furnishings Inc. v. Zen Path LLC*.

As reported at 81 BNA's PTCJ 293, on December 23, 2010 the U.S. District Court for the Eastern District of California ruled that a company selling furniture online was entitled to a preliminary injunction barring a competing company from sending DMCA takedown notices. *Design Furnishings Inc. v. Zen Path LLC.*

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

As reported at 81 BNA's PTCJ 24, on October 27, 2010 the U.S. District Court for the District of Nevada ruled that redirecting reservations to Expedia was cybersquatting, infringed hotel's marks. *New York-New York Hotel & Casino v. Katzin*.

As reported at 81 BNA's PTCJ 346, on January 12, 2011 the U.S. District Court for the Western District of Washington ruled that evidence that defendant taught others how to exploit Microsoft Corp. trademarks to increase website traffic, and sold software to systematize this endeavor, will support contributory cybersquatting and dilution claims. *Microsoft Corp. v. Shah.*

As reported at 96 USPQ 2d 1674, on September 8, 2010 the U.S. District Court for the Eastern District of California ruled that claim asserted by owner of building materials company for false designation of origin, based on defendant search engine provider'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", is dismissed, since plaintiff has failed to allege how defendant's use of term creates misleading suggestion as to producer of plaintiff's goods, and any confusion that may arise as to plaintiff's affiliation with sponsored link, or as to trademark status of "Styrotrim", does not constitute confusion as to producer of goods. *Jurin v. Google Inc.*

As reported at 96 USPQ 2d 1884, on February 26, 2010 the U.S. District Court for the Eastern District of Michigan held that plaintiff asserting claim for violation of Anticybersquatting Consumer Protection Act has not established that defendants had bad faith intent to profit in registering "careeragentsnetwork.biz" and "careeragentnetwork.biz" internet domain names, which contain plaintiff's claimed "Career Agents Network" mark and are used for "gripe" websites critical of plaintiff's business practices; use of plaintiff's alleged mark in domain names registered to criticize plaintiff's business is not "inconsistent with", or in violation of, ACPA. *Career Agents Network Inc. v. careeragentsnetwork.biz*.

As reported at 81 BNA's PTCJ 253, on December 14, 2010 the U.S. District Court for the District of Utah held that invisible AdWords were a use in commerce but noninfringing, absent a likelihood of confusion. *1-800 Contacts Inc. v. Lens. Com Inc.*

As reported at 97 USPQ 2d 1134, on July 12, 2010 the U.S. District Court for the Northern District of California ruled that defendant's argument that plaintiff has failed to plausibly allege that defendant "used" plaintiff's "Intel" mark, and that plaintiff thus has failed to state claim for infringement, has some merit; however, dismissal of complaint on this ground would be premature, since defendant's use of arguably redundant term "intel" in its "Americas News Intel Publishing" service could be viewed as effort to free-ride on plaintiff's mark. *Intel Corp. v. Americas News Intel Publishing LLC.*

As reported at 81 BNA's PTCJ 254, on December 13, 2010 the U.S. District Court for the District of Utah held that AdWords advertiser could not defeat a claim of trademark infringement by arguing that the plaintiff had engaged in the same activities. *1-800 Contacts Inc. v. Memorial Eye P.A.*

As reported at 81 BNA's PTCJ 431, on January 25, 2011 the U.S. District Court for the Central District of California ruled that a survey showing that some users who conducted a Google search using a registered term believed that they were being lead to the trademark owner's website, as well as other evidence establish actual confusion arising from Google keyword ad. *Binder v. Disability Group Inc.*

As reported at 80 BNA's PTCJ 693 on September 13, 2010 the U.S. District Court for the Central District of California found a likelihood of success for claims related to purchasing keyword triggers for online advertising and other online uses. The court also ruled that the owner of a registered trademark had established a likelihood of success on the merits of a claim of infringement based on the tagging of a video posted on the YouTube video clip website. *Partners for Health and Home L.P. v. Yang*.

As reported at 97 USPQ 2d 1364, on May 19, 2010 the U.S. District Court for the Western District of Washington ruled that defense of nominative fair use is appropriate if defendant uses plaintiff's mark to describe plaintiff's product, even if defendant's ultimate goal is to describe its own product; in present case, defendants' use of "Hendrix" in URLs and business names does not constitute nominative fair use of plaintiffs' "Hendrix" family of marks, since defendants' use of "Hendrix" to describe their own product, namely, marketing and licensing of goods related to late musician Jimi Hendrix. *Experience Hendrix LLC v. HendrixLicensing.com Ltd.*

As reported at 97 USPQ 2d 1454, on August 27, 2010 the U.S. District Court for the Southern District of Ohio granted plaintiff state university combined temporary restraining order and preliminary injunction prohibiting defendants from using plaintiff's various "Buckeyes" and "Ohio State" trademarks on websites or in electronic and printed publications, since plaintiffs have demonstrated strong likelihood of success on merits of their infringement and unfair competition claims, since plaintiff will suffer irreparable harm if defendants continue to publish and disseminate their products, and since balance of harms and public policy concerns favor grant of injunction. *Ohio State University v. Thomas*.

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

As reported at 81 BNA's PTCJ 492, on February 11, 2011 the U.S. District Court for the Eastern District of Michigan ruled that the former employee of a DNA-analyzing software company is not liable for stealing the company's trade secrets under Michigan's Uniform Trade Secrets Act. *Gene Codes Corp. v. Thomson*.

TRADE DRESS/COPYRIGHT – *Case Law* – U.S. District Courts

As reported at 81 BNA's PTCJ 493, on January 6, 2011 the U.S. District Court for the Middle District of Pennsylvania ruled that mimicking an iPhone app's "look and feel" could amount to trade dress and copyright infringement. *Hershey Co. v. Hottrix LLC*.

FALSE ADVERTISING – *Case Law* – U.S. District Courts

As reported at 96 USPQ 2d 2008, on July 23, 2010 the U.S. District Court for the District of Delaware ruled that plaintiffs have failed to satisfy their burden, for preliminary injunction purposes, of showing, literal falsity of statement on defendant's comparative advertising blog averring that plaintiffs' dietary supplements consist of "99% additives", since statement is largely correct, and defendant did not state that additives in question are harmful or render plaintiffs' products inferior. *QVC Inc. v. Your Vitamins Inc.*

PATENTS – U.S. Patent and Trademark Office

As reported at 81 BNA's PTCJ 248, on December 16, 2010 the Patent and Trademark Office announces a plan to open its first satellite office for patent operations in Detroit within a year. PTO Director David J. Kappos says that the Detroit office will house 100 examiners and some support personnel.

TRADEMARKS – U.S. Patent and Trademark Office

As reported at 81 BNA's PTCJ 180, on November 29, 2010 the Trademark Trial and Appeal Board affirms refusal to register "NANDrive" for flashdrives based on genericness. *In re Greenliant Systems Ltd.*

As reported at 81 BNA's PTCJ 260, on November 30, 2010 the Trademark Trial and Appeal Board reverses ruling that "thumbdrive" is generic for USB flash drive devices. Proposed "Thumbdrive" trademark is not generic term for applicant's "flash drive" data storage devices and related software, since evidence showing some generic use is offset by evidence showing significant amount of both proper trademark use and trademark recognition. *In re Trek 2000 International Ltd.*

As reported at 81 BNA's PTCJ 343, on January 10, 2011 Microsoft files a motion with the Trademark Trial and Appeal Board opposing Apple Inc.'s attempt to register the term "App Store" for its online store where users can download applications for use on an iPod, iPad, or iPhone. *Microsoft Corp. v. Apple Inc.*

France – Foreign Courts

As reported at 81 BNA's PTCJ 153, on November 25, 2010 the Paris Court of Appeals ruled that Google did not infringe a French bedding manufacturer syndicate's trademark by selling keywords associating the trademark with links sponsored by the syndicate's competitors. *Google France v. Syndicat Francais de la Literie*. ■

Mission Statement—Information Technology Law Section, State Bar of Michigan

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:

- the protection of intellectual and other proprietary rights;
- 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;
- electronic commerce
- electronic implementation of governmental and other non-commercial functions;
- the Internet and other networks; and
- associated contract and tort liabilities, and related civil and criminal legal consequences. ■

The *Michigan IT Lawyer* is pleased to present "The Pitfalls of an Internet Persona: Evidentiary and Privacy Concerns of Online Social Media" by Kate Mercer-Lawson. Ms. Mercer-Lawson is one of three student authors to receive a 2010 Edward F. Langs Writing Award from the State Bar of Michigan's Information Technology Law Section. 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!

The Pitfalls of an Internet Persona: Evidentiary and Privacy Concerns of Online Social Media

By Kate Mercer-Lawson*

Introduction

When a person hits "send" after writing an email or "publish" after typing a MySpace post, it is doubtful that she contemplates this communication being used to implicate or even help convict her of a crime. Nevertheless, "once the transmissions are received by another person, the transmitter no longer controls its destiny"[1] to the extent that it may become relevant evidence in a court of law. Relevant evidence means "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."[2] However, even relevant evidence can be deemed inadmissible at trial if a balancing test finds "its probative value . . . substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury . . . or needless presentation of cumulative evidence."[3] Trial courts enjoy broad discretion in determining the value of evidence and whether it is unfairly prejudicial.[4]

According to Loyola Law School Dean Victor Gold, courts do this balancing because eventually, lay fact finders must cognitively process evidence to reach a decision.[5] Evidence that dominates "the decisionmaker's perceptions, memory and imagination"[6] tends to influence the decision making process strongly.[7] Additionally, as Gold suggests, "the most significant factor influencing the memorability and hence the availability of evidence is its vividness."[8] Evidence is "vivid" when it is personally relevant to a juror.[9] Using and interpreting information from online social media is personally relevant to many people today,[10] so it is certainly "vivid" by Gold's standard. Furthermore, because jurors often expect vivid evidence to be determinative at trial,[11] courts frequently encounter issues with online social media as they make admissibility decisions.[12] They must guard against prejudice, which, according to Gold, results "when . . . vividness exceeds the objective value of the evidence in question."[13]

The value of evidence is important because of the standard of proof parties must meet. A plaintiff in civil court must generally establish her prima facie case by a preponderance of the evidence,[14] which "simply means 'the greater weight of the evidence.'"[15] In criminal proceedings, evidence rules take on special significance due to the elevated standard of proving conduct beyond a reasonable doubt,[16] which is doubt arising "from the evidence, the lack of evidence, or a conflict in the evidence."[17] Evidence arising from online social media has the potential to introduce significant doubt and conflict because it is usually demonstrative, which means "principally used to illustrate or explain other testimonial, documentary, or real proof, or a judicially noticed fact."[18] This type of evidence does not normally rise to the level of probative evidence, which is "[t]estimony carrying quality of proof and having fitness to induce conviction of truth, consisting of fact and reason co-operating as co-ordinant factors."[19] However, the Indiana Supreme Court's recent holding in *Clark v. State*[20] indicates that at least in Indiana, social media's probative value is gaining recognition and stimulating debate.

This Note discusses online social media in the context of evidence rules and privacy rights, with a focus on Indiana rules and case law. Part I explains and emphasizes the importance of the Indiana Rules of Evidence that have the greatest bearing on online social media evidence: rules involving relevancy, hearsay, authentication, and the "best evidence rule." Part II explores the implications of *Clark v. State*,

which allowed a criminal defendant's social media persona into evidence despite glaring concerns.[21] Part III discusses the intersection of evidence, the Internet, and the right to privacy, particularly as it has incited administrative and legislative action. Finally, Part IV advocates for amendments to the Indiana Rules of Evidence to address the evolution of technology and the potential for violating an individual's common law and constitutional right to privacy.[22]

Indiana Rules of Evidence Pertaining to Electronically Stored Evidence

Legal scholars specializing in evidence view online evidence as one of the key challenges in recent years.[23] Online evidence is a difficult topic because rules of evidence "do not expressly refer to electronic evidence or electronically stored information. Nonetheless, the rules are regularly used to admit these forms of evidence."[24] In Indiana, the rules commonly used to admit electronic evidence in litigation are the rules regarding relevancy, hearsay, and authentication.[25] The "best evidence rule" (as expressed in Rules 1002[26] and 1004[27]), although rarely invoked to challenge online evidence,[28] is also pertinent because it requires attorneys to submit original or acceptable secondary pieces of evidence at trial.[29] The "best evidence rule" also provides insight as to the intricacies of admitting evidence that involves state-of-the-art technology.[30] Because technology tends to zoom ahead of the law in terms of progress and change,[31] the Indiana Rules of Evidence may be courts' major guide until a significant body of online social media evidentiary case law accumulates. Indiana courts should heed the rules on relevancy, hearsay, authentication, and "best evidence" closely in the interim to avoid unduly prejudicial and overly invasive results.

Relevancy and Its Limits

The Indiana Supreme Court recognizes the importance of demonstrative evidence and has ruled that "demonstrations are permitted . . . during a trial if they will aid the court and the jury."[32] Relevancy is critical to any discussion of demonstrative online social media evidence in litigation because this type of evidence is ubiquitous today, yet relevant in far fewer situations. For instance, photographs are generally relevant and admissible in Indiana courts "only where they will assist and enlighten the jury . . . [and] . . . are not proper where they may serve as a source of confusion or prejudice."[33] Because written and oral evidence can clearly be as demonstrative as visual evidence, the Rules provide guidance as to its admissibility as well.

Rule 402 of the Indiana Rules of Evidence provides that all relevant evidence is admissible in court except as otherwise indicated by the United States Constitution, the Constitution of the State of Indiana, or other Indiana statutes and rules of court.[34] The converse of the rule is that non-relevant evidence is inadmissible.[35] Rule 401 sets the scope of the term "relevant" such that the material offered as evidence must have probative value toward the merits of a party's case.[36] The exclusionary factors listed in Rule 403—prejudice, confusion, and unfair delay—address the fairness and efficiency approaches inherent in deciding which among a slew of exhibits may go before a court.[37]

In America's adversarial legal system, evidentiary concerns are paramount to an efficient result.[38] Seventh Circuit Judge Richard Posner has argued that "the rules of evidence enable the judge . . . to ameliorate the problem of socially excessive evidence search, while at the same time the rules governing burden of production enable him to ameliorate the problem of socially insufficient search."[39] The two prongs of Rule 404 provide guidance on sufficient searches for character evidence—that is, what personal information may be offered about an individual.[40] According to Rule 404(a), the default rule is that character evidence is not generally admissible "for the purpose of proving action in conformity therewith on a particular occasion."[41] Rule 404(b) provides that "[e]vidence of other crimes, wrongs or acts is not admissible to prove the character of a person in order to show action in conformity therewith."[42] In other words, an attorney may not use evidence of other crimes to support the logic that correlation equals causation.[43] Evidence of the 404(b) variety is only admissible in a limited range of situations: to show "proof of motive, intent, preparation, plan, knowledge, identity, or absence of mistake or accident."[44] Moreover, the prosecutor must provide reasonable pre-trial notice of the nature of this evidence upon the request of the defendant.[45]

Indiana's highest court adopted Rule 404(b) from the Federal Rules of Evidence in the 1992 decision *Lannan v. State*[46] with the goal of allowing the state to "present evidence that completes the story of the crime in ways that might incidentally reveal uncharged misconduct."[47] The *Lannan* court cautioned that evidence of previous actions examined[48] under the rule "must be so similar, unusual, and distinctive as to earmark them as the acts of the accused."[49] Indiana now refers to this rule as the "forbidden inference rule."[50] The rationale behind Indiana's view of Rule 404(b) surfaced in *Bassett v. State*,[51] where the Indiana Supreme Court held that "evidence of extrinsic offenses poses the danger that the jury will convict the defendant because his 'general character' is bad or . . . he has a tendency to commit other crimes."[52]

Indiana's Rule 404(b) is identical to its federal counterpart except that the federal version specifies that evidence

of other crimes, wrongs, or acts may be admissible to show "proof of motive, *opportunity*, intent, preparation, plan, knowledge, identity, or absence of mistake or accident."[53] By comparison, Indiana's version of the rule does not include the word "opportunity."[54] Generally, Indiana courts and legal commentators have believed that leaving "opportunity" out of this rule is not a problem.[55] The list of exceptions in Rule 404(b) is not exhaustive[56] because the Indiana Supreme Court intended the rule to be inclusionary, not exclusionary.[57] Furthermore, because extrinsic act evidence can be admitted for other purposes than to prove character in conformity with a crime,[58] the literal omission of "opportunity" "does not affect admissibility of extrinsic act evidence offered to show opportunity."[59] After all, as the Indiana Supreme Court noted in *Kubsch v. State*, "otherwise inadmissible evidence may become admissible where the defendant 'opens the door' to questioning on that evidence."[60] Some courts and commentators[61] suggest that although Indiana does not list opportunity in Rule 404(b),[62] "it evidently is intended to cover all or a part of a category called 'capacity' . . . and has been applied in similar circumstances."[63] Yet the Indiana Supreme Court's decision in *Clark v. State*[64] indicates that even without "opportunity" explicitly noted in this rule, courts still tend to consider evidence that would involve the defendant's opportunity to commit the crime.[65] When "opportunity evidence" involves online social media, courts may face a host of unpleasant questions as to why it was relevant in the first place.

Hearsay

In addition to relevancy, the hearsay rules are particularly important in modern litigation because so many individuals, including potential parties to a suit, make statements online every day via blogs, forums, chats, and emails. The "800 Rules" of evidence cover the somewhat murky area of hearsay: "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[66] A "statement" is either "an oral or written assertion" or "nonverbal conduct of a person, if it is intended by the person as an assertion."[67] The general rule—that hearsay is inadmissible[68]—is necessarily riddled with qualifications and exceptions.[69] One such exception is "non-hearsay" material described in Rule 801(d)(2)(A): "a statement is not hearsay if . . . [it] is offered against a party and is the party's own statement, in either an individual or representative capacity."[70]

Applying hearsay exceptions is challenging because of the potential to confuse issues at trial. Creighton University School of Law Professor G. Michael Fenner notes with respect to hearsay that "if evidence confuses the issue[,] then it makes it more difficult for the jury to keep focused on the real issues, which . . . risks an outcome based on the resolution of false issues."[71] Furthermore, the analysis becomes more cumbersome as multiple levels of hearsay amass.[72] This problem is foreseeable in the realm of online social media, where content is rarely as simple as one simple statement on a web page. Therefore, if hearsay is present in an online form, courts must "analyze whether each piece of hearsay conforms with an exception to the hearsay rule,"[73] a burdensome task.

Authentication

The third area of concern for online evidence and admissibility can be found in the "900 Rules," which deal with the requirement of authentication. For online evidence, authenticity becomes complicated and less reliable than it would be for photographs or other media because the Internet is not a static medium.[74] Simply stated, authentication requires an individual offering an item into evidence to demonstrate "that the matter in question is what its proponent claims."[75] Rule 901(b) provides a litany of illustrations as to what constitutes authentication—including, but not limited to, voice identification, handwriting analysis, or distinctive appearance.[76]

Material that can change in milliseconds would seem exceedingly hard, although certainly not impossible, to authenticate. Constantly monitoring online content would be cost-prohibitive for most Internet service providers ("ISPs"), ultimately manifesting in both inflated prices for consumers and the tendency toward excessive removal of site content.[77] This "ISP overdeterrence phenomenon"[78] is bolstered by the observation in the communications law community that "perhaps service providers . . . [once] had the ability to keep a watchful eye over their customers' Web pages, but the immense size of the Web today makes such supervision almost impossible."[79] The problem lies not only in monitoring content, but also in balancing the competing interests of policing user misconduct and encouraging the growth of online social media.[80]

Online evidence is also problematic because it is "hackable;"[81] that is, any number of anonymous users may make representations that appear to be, but are not, someone else's words.[82] The U.S. Department of Justice has recognized this problem publicly, noting in a recent report that "[criminal justice] first responders must understand that computer data and other digital evidence are fragile. Only properly trained personnel should attempt to examine and analyze digital evidence."[83] Furthermore, this type of evidence—especially from social networking sites—can be

unreliable because of relative anonymity and the problems involved in "establish[ing] the veracity of communications sent by third parties."[84] Robert Kelner, co-chair of the New York County Lawyers civil trial practice course emphasizes this point, asserting that "[n]o Web site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation."[85] To complicate the matter, many courts presented with electronic evidence "essentially . . . [bypass] authentication requirements altogether, asking only that the foundation requirements of the applicable hearsay exception be proven."[86] The result seems to be that admissibility of online statements always rests on a case-by-case determination—or, as evidence expert John Henry Wigmore suggests, that it "does not result in abstract rules; each ruling stands by itself, and can form no precedent."[87] Sometimes, as detailed in the discussion of *Clark v. State*,[88] this case-by-case method of admitting evidence opens the door to debate on proper trial procedure and the implications of these procedures on the right to privacy.

The "Best Evidence Rule"

Ultimately, courts must also weigh proffered evidence in terms of whether it satisfies the "best evidence rule." The rule is embodied in Rule 1002[89] of the Indiana Rules of Evidence and articulated in *Purifoy v. State*,[90] in which the defendant challenged a detective's testimony that he discovered the defendant's actions on a computerized database. Dealing with the "requirement of original,"[91] the rule stipulates that unless otherwise addressed by state law or the rules of evidence, the original piece of evidence must be used to verify its contents in court.[92] Among others, some of the main purposes of the rule are to "check fraud and guard against innocent misidentification."[93] The text of Rule 1002 emphasizes writings and recordings[94] as the "best evidence" to submit, and Rule 1001(a) refines this concept by stating that "letters, words, sounds, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation" suffice.[95] And in Indiana, according to *Hape v. State*,[96] these desirable pieces of evidence must be properly authenticated under Rule 901(a) in order to be admissible.[97]

Still, in *Purifoy*, the Indiana Court of Appeals rather summarily dismissed the defendant's claim that the State should have provided a writing or recording from the computerized database that allegedly identified him as a certain pawnshop customer.[98] The court reasoned that the State had no way to present this so-called "best evidence" on appeal.[99] Moreover, the court ruled that even if the trial court had erred in allowing testimony regarding the computerized data "and even if it slightly prejudiced Purifoy," that error would not overcome the appellate standard of review;[100] it was not "such a blatant denial of fundamental due process so as to require reversal" of the trial court's decision.[101] Whether the court intended to do so or not, this callous treatment of the "best evidence rule" arguably muddied the waters in the years prior to *Clark v. State*.[102]

The Indiana Supreme Court's Decision in Clark v. State: Against Evidentiary Common Sense

On October 15, 2009, the Indiana Supreme Court issued its opinion in the case of *Clark v. State*.[103] Pursuant to Indiana Rule of Appellate Procedure 4,[104] Ian Clark's case came to the state's court of last resort on direct appeal from the Kosciusko Circuit Court, where a jury had found him guilty of murdering his fiancée's two-year-old daughter and the court sentenced him to life in prison without parole.[105] The sordid facts certainly supported this verdict and sentence—Clark's fiancée returned from work to find her daughter "naked and blue" and "brain dead" according to Clark, who refused to make a 911 call on behalf of the girl.[106] Police officers who arrived on the scene to arrest Clark and transport the family to the hospital found an equally horrifying scene that included numerous blood spatters and a hole in a wall containing blood and hair that was confirmed as the child's.[107] The child had suffered devastating contusions and broken bones before she died, and her blood was all over Clark's shirt.[108] Clark's comments immediately following his arrest were as chilling as the crime of which he would be convicted; he told a detective, "I will send the Hell's Angels to kill you . . . it's only a C felony. I can beat this." On the facts alone, Clark's case was not particularly noteworthy. The crux of his defense was that his state of mind during the alleged crime was reckless rather than criminal.[110] What caught the attention of the Indiana Supreme Court was the electronic evidence introduced to the jury—evidence introduced in order to determine Clark's state of mind at the time of the alleged homicide.[111] The novel issue before the court seems inevitable in a digital world: "should the trial court have permitted the State to offer into evidence Clark's entry from the social networking website MySpace?"[112] The contentious piece of evidence was an online posting visible on Clark's MySpace.com[113] profile page, ostensibly to describe himself:

> Society labels me as an outlaw and criminal and sees more and more everyday how many of the people, while growing up, and those who judge me, are dishonest and dishonorable. Note, in one aspect I'm glad to

> say I have helped you people in my past who have done something and achieved on the other hand, I'm sad to see so many people who have nowhere. To those people I say, if I can do it and get away. B ... sh.... And with all my obstacles, why the f ... can't you.[114]

Like the Kosciusko court before it, the Indiana Supreme Court held that this electronic evidence was indeed admissible.[115] Clark's counsel argued that Rule 404(b), which precludes admissibility of "evidence of other crimes, wrongs, or acts . . . to prove the character of a person,"[116] should have excluded the posting, but the court rejected the argument because Clark had put his state of mind at issue.[117] Finding no violation of due process or other fundamental error, and perhaps also considering the State's burden of proving mens rea, Chief Justice Shepard wrote, "Inasmuch as Clark seemed eager to discuss the subject and the court took such action as defense counsel requested, we see no error."[118]

Immediately following the Clark decision, the Indiana Supreme Court Committee on Rules of Practice and Procedure questioned the court's reasoning.[119] One problem with the opinion is the apparent confusion of Rule 404(a)—the "general character evidence rule"[120]—and Rule 404(b).[121] The court discussed the MySpace posting in the context of Rule 404(b)[122] but essentially treated the pertinent clauses as evidence "of a pertinent trait of character offered by an accused, or by the prosecution to rebut the same,"[123] which falls under Rule 404(a).[124] The two clauses that could have been dispositive were "[s]ociety labels me as an outlaw and criminal"[125] and "I'm glad to say I have helped you people in my past."[126] Both parts of the posting were vaguely worded and, as the State noted at trial, were "solely evidence of . . . [Clark's] own statements, not of prior criminal acts."[127] Yet even assuming the court intended to admit the postings under Rule 404(a)(1), it is quite a stretch to classify these boastful words as evidence of a "pertinent trait of character."[128] Clark's statements suggest an overinflated ego, but they fall short of the plain meaning of pertinent: "pertaining to the issue at hand,"[129] which was whether he had in fact caused the death of his fiancée's child with a criminal state of mind. The posting could just as easily be viewed as bravado, and even if it had been the only available piece of evidence against Clark, it should not have been deemed relevant.

The issues of hearsay and authentication in *Clark* also merit discussion. Based on the trial record,[130] Clark's MySpace posting arguably fell within the ambit of Rule 801(d)(2)(A), as a party's own statement, and was not inadmissible hearsay. The hearsay rules, however, are only one subset of the rules of evidence, and the fact that hearsay rules did not bar the evidence does not mean the evidence was otherwise admissible. Put otherwise, although Clark's statements were not inadmissible hearsay under Rule 801(d)(2)(a), they were still not admissible character evidence under Rules 404(a) or 404(b) and were therefore not relevant. Nor should the fact that Clark did not dispute the authenticity of his profile[131] have indicated that the condition precedent of authentication was met at trial. In fact, the opinion leaves the matter of authenticity in question by noting that "it seems that Matara [Clark's fiancée] *had helped Clark create his own personal entry on MySpace*."[132] Including this detail in the opinion begs the following question: Why did the court not, for example, require the illustration set forth in Rule 901(b)(1)—testimony of Matara, who was arguably a witness with knowledge that the matter was what proponents claimed it to be?[133] Thus, *Clark* also raises "the unique evidentiary issue . . . [concerning] the type and quantum of evidence necessary to make that identification or to permit the finder of fact to do so."[134] Even a tenuous attempt to authenticate the MySpace posting by clearly identifying the post's author would arguably have made it less disconcerting as a piece of admissible evidence.

The result in *Clark* is also troubling because the Indiana Supreme Court has not always been so generous with MySpace postings as probative evidence.[135] As an example, in *A.B. v. State*, a fourteen-year-old girl appealed multiple counts of delinquency for several MySpace postings she authored that would have constituted criminal harassment[136] if she had been an adult.[137] The Indiana Supreme Court reversed her adjudication as delinquent, saying that critical online evidence was too "sparse, uncertain, and equivocal."[138] This case was like *Clark* in that the defendant had made provocative comments on a MySpace profile and on group pages.[139] The court was concerned about the use of MySpace evidence because "[n]o expert witnesses were called" and "neither of the witnesses . . . [called] provided knowledgeable and reliable details about MySpace."[140] Furthermore, the court took a more common-sense approach to the MySpace issue, noting that although "A.B. had a subjective expectation that her words would likely reach [her school principal] . . . this alone . . . [did] not establish the intent element specified" in the statute.[141] The court also based its dismissal of the counts on the idea that "it . . . [was] even more plausible that A.B. . . . merely intended . . . to generally vent anger for her personal grievances."[142] In short, the approach taken in *A.B.* seems much more in line with proper evidentiary procedure than the approach taken in *Clark* because the *A.B.* court arguably considered why the evidence might or might not have been relevant, pertinent, or authentic.

Privacy Considerations Dealing with Online Social Media

Despite the brevity of the court's opinion, *Clark* is worthy of discussion because its evidentiary issues should concern citizens who value their privacy rights, particularly in this era of cloud computing.[143] The concept of cloud computing entails "the idea that . . . [a] computer's applications run somewhere in the 'cloud,' that is to say, on someone else's server accessed via the Internet."[144] As the Information and Privacy Commissioner of Ontario has observed, one's identity in the realm of cloud computing is complicated because a person is no longer identified by a single number.[145] In the past, people tended to think of their Internet identity in terms of the Internet Protocol or "IP" address only, which was like their personal computer's mailing address or phone number.[146] However, online identity today "is no longer a single number . . . but rather comprises a set of attributes including address, birthdate, degrees held, and personal preferences. Such personal information requires special protection, not only to prevent fraud and identity theft, but also to comply with privacy laws."[147] Since maintaining any Internet persona necessarily involves sharing this personal information with an unknown audience, many users are increasingly concerned about how their constitutional right to privacy is implicated on the Web.[148]

The concept that "individuals self-select through their online behavior . . . [and] generate information that is valuable to potential advertisers,"[149] although rooted in consumer law, also raises the question of whether this "self-selection" can waive one's privacy rights and open the door to these activities being used against them in almost any situation. In particular, employing liberal privacy policies to gather evidence about an individual is a sticky area because, according to the National Institute of Standards and Technology,[150] "disclosure of . . . [personally identifiable information][151] can seriously impact both individuals, by contributing to identity theft, and the organization, by reducing public trust in the organization."[152] Decisions involving whether an individual's online behavior can be monitored and used to convict him "must be balanced with the potential to infringe on the suspect's constitutional and common law rights, particularly when law enforcement and the responsibility of national security are taken into consideration."[153]

Constitutional and Common Law Bases for the Right to Privacy

The constitutional right to privacy as we know it originated in *Griswold v. Connecticut*,[154] in which the Supreme Court ruled that "specific guarantees in the Bill of Rights have penumbras . . . [and] various guarantees create zones of privacy."[155] The right as defined by the Court is a substantive due process interest created by guarantees from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.[156] Although discussion of the right originally stemmed from the then-provocative question of whether husbands and wives could use birth control in the private realm of the marital bedroom,[157] it has come to encompass "the right to define one's own concept of existence, of meaning, [and] of the universe."[158]

The high priority given to privacy is also evident in the common law.[159] The Restatement (Second) of Torts recognizes "privacy torts" such as the invasion of privacy, which imposes liability for an individual who intentionally invades another's private affairs.[160] "Publicity given to private life" is another example of a privacy tort; "one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized . . . is not of legitimate concern to the public."[161] These causes of action are subject to a reasonableness standard[162] and carry certain limitations. For instance, the Restatement drafters clearly contemplated that "voluntary public figures"—individuals who place their lives under scrutiny by assuming leadership roles or public submission of their work—are not afforded the same generous common law privacy right.[163] The voluntary public figure who "(submits) himself or his work for public judgment, cannot complain when he is given publicity that he has sought, even though it may be unfavorable to him."[164] In other words, not everyone has a reasonable expectation of privacy.

Involuntary public figures—individuals whose only manifestation of consent to publicity of their words and actions is their conduct—are also not contemplated as having the same privacy rights as others even if they do not understand the nature of their rights.[165] Many persons involved in public litigation fall squarely within this category because their alleged conduct subjected them to litigation,[166] and public policy concerns tend to motivate more transparency where adversarial disputes are concerned. As the Supreme Court observed in *United States v. Karo*, "two people who speak face to face in a private place . . . both may share an expectation that the conversation will remain private, but either may give effective consent to . . . surveillance" of that communication.[167] Moreover, as the Restatement notes, "those who commit . . . [crimes] or are accused of [them] . . . may make every possible effort to avoid it, but they are nevertheless persons of public interest, concerning whom the public is entitled to be informed."[168] People who cultivate Internet

personae, from bloggers to those who merely "chat" online, can just as easily fit into this category. If they attempt to raise invasion of privacy claims relating to Internet content, they may be rudely awakened by the requirement that they prove a reasonable expectation of privacy.[169]

Regardless of someone's status as a "voluntary public figure," "involuntary public figure," or neither, the Supreme Court has stated a twofold requirement when an individual wishes to assert her privacy rights.[170] A person must show both a subjectively reasonable and an objectively reasonable—"one that society is prepared to recognize as 'reasonable'"[171]—expectation that the communication be kept private rather than seized as evidence. The *Katz* Court was comparing phone call participants' expectations of privacy to those they might enjoy in their homes, reasoning that

> a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[172]

In light of the Internet's current primacy in American culture and the very public nature of many online communications, perhaps "it is unrealistic to believe that an individual's expectation of online privacy exceeds or even equals . . . [her] expectation of privacy within . . . [her] own home."[173] Although most online conduct probably does take place in people's homes, online "customs" of individuals willingly using unsecured wireless connections, companies using tracking "cookies" on their websites, and employers monitoring at-work Internet use may be clear indicators of a general decline in privacy expectations for all Internet-based communication.[174]

Developments in Other Jurisdictions

The prevalence of online social media and the above-mentioned changes in privacy expectations[175] raise the question of whether anyone who has an Internet persona is a "voluntary public figure"[176] according to the parlance of the Restatement of Torts. In many jurisdictions, what an individual posts on the Internet can indeed make her a "voluntary public figure"[177] or at least eliminate any reasonable expectation of privacy. In 2009, the Minnesota Court of Appeals considered the question of whether a MySpace posting is a private or public communication in *Yath v. Fairview Clinics*[178] and concluded that "the determination does not depend on whether the content offered through the medium is of general interest to the public, but on whether the content is conveyed through a medium that delivers the information directly to the public."[179] Perhaps the *Yath* holding implies that in Minnesota, participating in online social media is per se putting content at issue and subjecting it to censure or attention of the state authorities.

Minnesota is also an excellent example of how state actors can pursue wrongdoers who may have made themselves "voluntary public figures" through online social media. The State of Minnesota's revenue agents are increasingly "mining" social networking sites like MySpace and Facebook to find tax evaders.[180] Similarly, Nebraska revenue officials often utilize Google to recover unpaid back taxes; "if a Google online search isn't productive, agents use the social sites or chat rooms in a last-chance hunt for their quarries."[181] However, due to ethical concerns about adding "friends" to one's social network for the sole purpose of investigating tax payments, revenue agents may only use information that is publicly available.[182]

Wisconsin is another state that has made great headway in using online social media to apprehend people who subvert the law of the land.[183] The Wisconsin Department of Natural Resources (DNR) has been known to use information found on popular sites like eBay and Craigslist to build cases against suspected offenders.[184] Recently, the state made its first ever arrest and conviction based on the Facebook video application and commentary features.[185] In 2009, Wisconsin DNR officials used a Facebook video posted by Adam Frame of himself and fellow defendant Dustin Porter engaged in illegal "deer-shining"—which involves illuminating a deer and shooting it[186]—as evidence to pursue charges against Frame and Porter in Wisconsin state court.

Even arms of the federal government actively use online social media to pursue legitimate aims. The Central Intelligence Agency (CIA) uses Facebook in "vetting" recruits and has Facebook pages for its various embassies.[187] Furthermore, the federal government keeps a record of all federal blogs,[188] and some officials have suggested keeping a record of all federal government pages on social networking sites.[189] Still, privacy concerns predominate at the federal level because so much falls under various agency umbrellas. A major response to these concerns has been at the administrative level, most notably through the Federal Trade Commission (FTC), which periodically publishes guidelines to assist various industries whose users may be "voluntary public figures" in self-regulating their online activities.[190]

Administrative Responses to Online Privacy Concerns

As online privacy law has developed in various jurisdictions, regulatory bodies have responded out of necessity. Online privacy protection became an increasing priority in the late 1990s due to the explosive growth of the Internet,[191] but it evolved as a self-regulating field, as demonstrated by the FTC's report to Congress in 1998.[192] At that time, the FTC contemplated that to protect the online privacy rights of adults, "industry efforts looked promising and legislation was unnecessary."[193] This optimistic view stemmed partly from comparative studies revealing that the European Union endorsed self-regulation in many information transactions.[194] In 2000, the FTC issued a report to Congress that identified a set of core fair information practice principles: notice, choice, access, and security.[195] This report, followed by a 2007 update adding enforcement as the fifth principle,[196] was a response to consumer concerns with online profiling, especially in the context of tracking Internet users' personally identifying information via social media and online behavioral advertising.[197]

The first of the FTC's fair information practice principles, notice, means that "data collectors must disclose their information practices."[198] The second principle, choice, means that individuals need some option as to "how personal information collected from them may be used for purposes *beyond which the information was provided*."[199] The third principle, access, means the right "to view and *contest* the . . . data collected about them."[200] The fourth principle, security, means that reasonable steps must be taken by online data collectors "to assure that information collected . . . is accurate and *secure from unauthorized use*."[201] Finally, the fifth principle, enforcement, suggests self-regulation, private remedies, and overarching regulatory schemes to prevent the other four principles from becoming "merely suggestive rather than prescriptive."[202] The FTC has even suggested a statutory scheme to govern collection of online information, reasoning that "private . . . [and government] remedies would help create strong incentives" for entities to protect citizens against unjust invasions of privacy.[203]

Subsequent FTC reports and initiatives reflect increasing concern with how information is collected from people's online activities.[204] A 2007 FTC-sponsored "town hall meeting" emphasized reasonable security, limited data retention for consumer data, and "affirmative express consent for material changes to existing privacy promises."[205] In 2009, the FTC made several revisions to user tracking principles.[206] Companies that track consumer data in nontraditional ways must develop their own methods of disclosing the tracking and giving the consumers the choice of being tracked for that stated purpose.[207] Moreover, they are limited to retaining data "only as long as necessary to fulfill a legitimate business or law enforcement need,"[208] again to protect respect for individuals' private lives whenever possible.

The Office of Management and Budget (OMB) has joined the FTC in paying increased attention to the practice of tracking user information on federal websites in constructing online policies.[209] Federal websites are required by law to post "clear and conspicuous notice" to users of whatever tracking technology the governmental agency employs.[210] They must also give users a "clear and understandable means" to opt not to be tracked based on their online activity[211] and are precluded from discriminating against people who opt out of tracking by giving them access to the same material as those who consent to be tracked, i.e., not conditioning website access on waiving certain privacy rights.[212] Furthermore, the OMB has invited comments on "the applicability and scope of . . . [a three-tiered] framework on [f]ederal agency use of third-party applications or Web sites," a category that includes social media sites like Facebook or even MySpace.[213] The OMB contemplates more stringent scrutiny as to the uses of such a framework, namely for "technologies within the tiers that have higher privacy risks associated with them."[214]

Similarly, in December 2008, leaders of the Federal Web Managers Council published a set of suggestions regarding online privacy concerns for the Obama administration.[215] The council urged the new administration to "direct agencies to use a standard disclaimer to display on social media sites where they publish content (i.e., the EPA's Facebook page or Twitter page)."[216] This type of disclaimer would inform users when they were no longer on federal websites and had moved to a website under the control of a private entity.[217] Like many other regulatory bodies, the council seems prepared to help ensure that rapid Internet growth need not mean the disintegration of privacy rights.

Congressional Activity in Online Privacy

Finally, the legislative branch of the federal government is waging its own battles in the war of security versus privacy. In April 2009, Congressman Rick Boucher urged a Subcommittee on Communications, Technology and the Internet Hearing that "one clear way Congress can promote a greater use of the Internet for access to information, e-commerce and entertainment is to assure Internet users a high degree of privacy protection."[218] Citing the desire to be "a driver of greater levels of Internet uses . . . not as a hindrance to them," he announced his intent "to develop legislation

extending to Internet users . . . assurance that their online experience is more secure" in 2009.[219] Based on these words, Boucher's efforts are not far removed from past Congressional efforts like the Children's Online Privacy Protection Act (COPPA) of 1998[220] or the Electronic Government Act of 2002.[221]

In 1996, background research conducted and published by the Center for Media Education indicated that young children do not understand the ramifications of revealing personal information on the Internet.[222] FTC studies in the remainder of the decade revealed that nearly ninety percent of 212 popular websites collected some form of information from children, yet not even twenty-five percent of these websites gave clear notice of a privacy policy.[223] One of COPPA's main purposes was therefore to require website operators "to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[224] The federal government is acting in its parens patriae interest, reflecting the legal tradition that the government may regulate some matters more stringently for children when it would not for adults.[225]

By contrast, the Electronic Government Act of 2002 was notable for its requirement of a privacy impact assessment (PIA) from each governmental agency that collects information on visitors to its websites.[226] According to the OMB, the PIA is conducted

> (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[227]

Specifically, the PIA must contain the following:

> what information is to be collected; why the information is being collected; the intended use of the agency of the information; with whom the information will be shared; what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; how the information will be secured; and whether a system of records is being created under [the Privacy Act of the United States Code].[228]

Each of the aforementioned laws bears repeating for future legislative efforts in online privacy. From COPPA, it is important to remember that the Internet is still relatively uncharted territory, even for adults, and perhaps all users consequently deserve some degree of notice as to what dangers exist when signing up for online social media. Even for participants in seemingly innocuous instant messaging, many courts rely on the concept of implied consent in that participants "knowingly" consent to the possibility that their communications in online social media might not remain private.[229] And from the Electronic Communications Act, privacy impact assessments[230] could provide great value to state agencies, especially law enforcement, in determining when online social media like instant messaging or blogs can be used to regulate conduct or become relevant in any courtroom proceeding.

Out of necessity, the "big players" in online social media sites have responded to the privacy concerns of the decade. Google, an Internet giant, uses software "to scan for keywords in users' emails which (can then be used) to match ads" related to a user's online activity and persona, i.e., emails, "G-chat" messages, and other communications.[231] Google pledges only to release information about a user outside the bounds of the company if it has

> a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.[232]

MySpace is similarly committed to the FTC-endorsed principles of notice and choice. The website strives to provide notice by ensuring that users "are informed about who is collecting (their) information, how and why the information is being collected . . . to the extent it differs from what is allowed" under the privacy policy.[233] However, MySpace also clearly disclaims responsibility for privacy practices of other sites that may be integrated with their services.[234] With respect to the choice principle, MySpace promises to obtain permission before using personally identifiable information in a way that was not originally contemplated by or disclosed to the user, except where necessary to "protect the safety and security of [u]sers of the MySpace [s]ervices or members of the public including acting in urgent circumstances . . . or . . . comply with the law or legal process."[235]

Notable in all of the above social media privacy policies is the idea of a law enforcement exception. This is sound

policy; securing the conviction of alleged offenders like Indiana's Ian Clark is arguably, if not certainly, a compelling state interest. Yet privacy rights advocates like Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC), disagree.[236] Rotenberg has openly criticized the law enforcement exception as being too broad.[237] In 2002, he urged the Senate that "for a privacy law to be effective, it is critical that . . . [law enforcement] exceptions be carefully drafted and as narrow as possible. In my opinion, the exception for disclosure to law enforcement agencies . . . is too broad."[238] Rotenberg and his allies would prefer legislators to "stay with the standard in other privacy laws"—that is, to require a federal or state warrant, court order, or administrative order before using information about an individual's online activity in law enforcement.[239] It appears, though, that his arguments did not carry the day based on the continued presence of law enforcement exceptions in online privacy policies.

A Challenge to the Indiana General Assembly: Rethinking the Rules

In a Fall 2009 "back to school" address to ninth grade students in Arlington, Virginia, President Barack Obama urged his audience, "I want everybody here to be careful about what you post on Facebook, because in the YouTube age, whatever you do, it will be pulled up again later somewhere in your life."[240] Stated even more simply in the legal community, "the rule of thumb is: if it's in the public domain, it's fair game."[241] Keeping in mind that most Americans may not consider Internet postings things they physically or verbally "do" that carry legal ramifications, I would advise the Indiana General Assembly to amend the state's evidence rules. Rule 801's definition of "statement"[242] should be clarified to provide notice that "oral or written"[243] applies to any manifestation made, whether aloud, on paper, or via the Internet. Another effective way to provide notice of online evidence admissibility would be to add a comment or illustration listing various "statements" (e.g., Facebook or MySpace profiles or posts) that are *not* protected under traditional notions of privacy rights and may be admissible as hearsay. Providing this type of notice in the state code would enable Internet users to choose how to structure their behavior if they hope to avoid needless litigation.

Because making accommodations for notice may not suffice, authentication of computerized evidence should also become a priority for the next amendments to the Indiana Rules of Evidence. The policy argument for this kind of amendment is already well stated in Facebook's privacy policy, which is frequently updated to reflect the site's exponential growth.[244] Specifically, Facebook warns users that when they use the site,

> You can control the visibility of most of the information you share on Facebook through the privacy settings *you select*. Certain categories of information . . . are considered publicly available, and therefore do not have privacy settings. You can limit the ability of others to find this information on third party search engines through your search privacy settings.[245]

Logically, if any online social media posting can potentially become disputed material in a lawsuit, there should be a similar commitment by the state legislature to clarify how it will determine that the available evidence is what it is purported to be. The ideal place for this type of amendment or addendum would be in Rule 901(b)(10), which currently provides that "any method of authentication or identification" given by the Indiana Constitution, Indiana Code, or Indiana Supreme Court satisfies the condition precedent of authentication.[246] Conversely, if Indiana intends to treat statements made via online social media as self-authenticated evidence,[247] as the Clark holding implies, this intent should be codified as well. Once again, this kind of legislative action would position Indiana as a state committed to fair litigation and respect for privacy—namely, by giving citizens a greater capacity to make informed decisions about online activity.[248]

Notwithstanding the allure of setting new precedent to harmonize evidentiary and privacy law, it is true that Indiana waited nineteen years to adopt a version of the Federal Rules of Evidence.[249] Reading the Indiana Rules of Evidence also indicates that a sizeable number of them are identical to their federal counterparts.[250] However, these observations need not cloud Indiana's potential to make a change. After all, as former Indiana Supreme Court Justice Krahulik wrote in *Modesitt v. State*,[251] it was only three decades ago that "the majority of jurisdictions in the United States adhered to the orthodox view regarding admission of prior statements . . . and . . . Indiana was one of the first jurisdictions to move away from this orthodox position."[252] The *Modesitt* court placed great weight on the perceived trend that Indiana trial and appellate courts had "confused the application and clouded the original purpose of"[253] Rule 801's definition of hearsay and ostensibly saw value in overturning old precedent. Perhaps Indiana lawmakers should consider changes to the Indiana Rules of Evidence as a way to remain faithful to their original purpose, as stated in Rule 102: "to secure fairness in administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained

and proceedings justly determined."[254] With the Seventh Circuit similarly committed to serving "the general purposes of the Federal Rules of Evidence[255] and the interests of justice,"[256] the task of renovating the Indiana rules might not be nearly as daunting because Indiana would have a model for action.

Indiana is well poised to forge ahead in the realm of authenticating online evidence based on its recent disposition of the issue in *Hape v. State*[257] for another mode of communication: text messaging. In March 2009, the Indiana Court of Appeals settled an apparent issue of first impression involving text messages under Rule 901, concluding that "in Indiana . . . text messages are subject to separate authentication before being admitted into evidence."[258] Hape appealed his case in part because text messages on his cellular phone were accidentally admitted into evidence[259] after law enforcement officers apprehended him with more than eight grams of methamphetamine.[260] The court decided that it was harmless error to have introduced Hape's text messages to a jury "in the context of the entirety of the evidence," referring to the large amount and packaging method of the methamphetamine found on Hape.[261] However, the court disagreed with Hape's argument that his text messages should not have been admissible or even discoverable[262] and reasoned as follows:

> Text messages are intrinsic to the cellular telephones in which they are stored. "Intrinsic," as defined by *Black's Law Dictionary*, means "[b]elonging to a thing by its very nature; not dependent on external circumstances; inherent; essential." We conclude that the text messages at issue here are part and parcel of the cellular telephone in which they were stored, just as pages in a book belong to the book by their very nature, and thus they are intrinsic to the telephone. Indeed, Hape concedes that "the messages are inextricable from the phones themselves."263

The court also pointed out that "turning on a device that is made to be turned on constitutes a permissible examination of . . . evidence."[264] Thus, the question from *Hape*—besides the issue of whether reading his text message violated his privacy rights when there was ample evidence to convict Hape[265]—is as follows: how, exactly, should Indiana specify the procedure for authentication of electronically stored information?

Amending Rule 901(b)(10) might not be Indiana's only approach to deal with the problem of authentication. In some jurisdictions, courts weighing electronic evidence's admissibility have simply turned to Rule 901(b)(1)[266] and concluded that "it may be authenticated by a witness with personal knowledge,"[267] although it is not a prerequisite "that the witness laying the foundation for the admissibility of computer records be the one who entered the data . . . or be able to attest personally to its accuracy."[268] In Maryland, for example, the *Lorraine* court relied on precedent from the Eleventh Circuit in *United States v. Siddiqui*[269] to support its contention that courts have relied on Rule 901(b)(4)—"appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances"[270]—throughout the decade to authenticate electronically stored information such as website content and text messages.[271] Furthermore, the opinion emphasized efforts by the United States District Court for the District of Maryland to set protocol for discovery of potentially relevant electronic evidence.[272] This federal district's attempts to identify workable techniques such as inserting "hash values" into data sets[273] demonstrate that Indiana would not be the first to contemplate change in this area. Perhaps more importantly, they indicate that new evidence-procuring policies can be instituted without being unreasonably intrusive, as demonstrated by the protocol sheet's emphasis on heeding what is "not reasonably accessible without undue burden or cost" as well as preventing "prejudice to any substantive right to assert, or oppose, waiver of any protection."[274] In other words, improved evidentiary procedures need not come at the expense of individual privacy rights.

Conclusion

In 1890, Samuel Warren astutely noted with eventual Supreme Court Justice Louis Brandeis in the *Harvard Law Review*,

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[275]

Citing new technology as the impetus for "the next step which must be taken for the protection of the person,"[276] Warren and Brandeis's argument is on point with today's jurists who, like Judge Joseph Tauro, believe "courts should adopt appropriate standards so that parties can obtain a remedy"[277] when privacy and evidentiary concerns collide. Although the tone is unclear from Judge Tauro's opinion as stated in *McMann v. Doe*,[278] his remark that "it is unreasonable to demand that the court system unmask every insolent,

disagreeable, or fiery anonymous online figure"[279] should serve as a cautionary reminder that the law must evolve along with technology.

As technology and the law concurrently develop, it is imperative that all branches of government take appropriate action to continue protecting the rights of the governed. If online social media evidence becomes the norm in courts of law, Indiana and other states must update their rules of evidence. Specifically, legislatures must pay close attention to how online evidence intersects with relevancy, hearsay, authentication, and "best evidence" rules. Decisions like *Clark* are not only useful cases for evidence courses, after all; they are also clear indicators of how online personae will be treated in society.

Furthermore, state efforts to update evidence rules are vitally important because of rapid changes in the realm of privacy law. Just as federal agencies, Congress, and major online entities are clarifying rights and responsibilities, Indiana must clarify to individuals how an online persona can be used against them in court proceedings. After all, the future leaders of Indiana "grew up in an age . . . of instantaneous communication and with it the need for new modes of thinking in the area of privacy."[280] It is my hope that today's state legislators feel and heed a duty to ensure that by the time the next generation takes over, it no longer "face[s] a realm of unfamiliar thinking about the meaning of digital privacy."[281] ■

Endnotes

* J.D. Candidate, 2011, Indiana University School of Law—Indianapolis; B.A., 2004, Indiana University, Bloomington, Indiana.

1 United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996).

2 Fed. R. Evid. 401; Ind. R. Evid. 401.

3 Ind. R. Evid. 403.

4 Matthews v. State, 866 N.E.2d 821, 825 (Ind. Ct. App.), *trans. denied*, 878 N.E.2d 206 (Ind. 2007).

5 Victor J. Gold, *Federal Rule of Evidence 403: Observations on the Nature of Unfairly Prejudicial Evidence*, 58 Wash. L. Rev. 497, 516 (1983) (using cognitive science concepts to suggest how decisionmakers perceive courtroom evidence).

6 *Id.*

7 *Id.* (citing R. Nisbett & L. Ross, Human Inference: Strategies and Shortcomings of Social Judgment 18-23 (1980)).

8 *Id.* at 518.

9 *Id.* (citing Nisbett & Ross, *supra* note 7, at 45-47).

10 *See* Press Release for Knowledge Networks, Internet Users Turn to Social Media to Seek One Another, Not Brands or Products (May 20, 2009), *available at* http://www.knowledgenetworks.com/news/releases/2009/052009_social-media.html (noting that 83% of Internet users ages 13 to 54 engages in online social media).

11 Gold, *supra* note 5, at 518 (noting that "jurors have been conditioned by television and motion pictures to expect a lawsuit to turn on some piece of vivid or dramatic evidence").

12 *See* Nathan Koppel, *Indiana High Court Allows MySpace Entry as Evidence in Murder Trial*, Wall St. J. Law Blog (Oct. 16, 2009), http://blogs.wsj.com/law/2009/10/16/indiana-high-court-allows-myspace-entry-as-evidence-in-murder-trial/.

13 Gold, *supra* note 5, at 520.

14 Andis v. Newlin, 442 N.E.2d 1106, 1108 (Ind. 1982).

15 Travelers Indem. Co. v. Armstrong, 442 N.E.2d 349, 361 (Ind. 1982) (quoting Great Atl. & Pac. Tea Co. v. Custin, 14 N.E.2d 538 (Ind. 1938)).

16 Palmer v. State, 411 N.E.2d 643, 646 (Ind. Ct. App. 1980) ("[O]f course, the duty of establishing a fact 'beyond reasonable doubt' imposes a duty far greater than to establish the same fact by 'a fair preponderance'") (quoting Kempf v. Himsel, 98 N.E.2d 200 (Ind. Ct. App. 1951)).

17 Kien v. State, 782 N.E.2d 398, 407 (Ind. Ct. App.) (quoting Chambers v. State, 551 N.E.2d 1154, 1156 (Ind. Ct. App. 1990)), *trans. denied*, 792 N.E.2d 47 (Ind. 2003).

18 Robert D. Brain & Daniel J. Broderick, *The Derivative Relevance of Demonstrative Evidence: Charting Its Proper Evidentiary Status*, 25 U.C. Davis L. Rev. 957, 968-69 (1992).

19 Nahmias Realty, Inc. v. Cohen, 484 N.E.2d 617, 621 (Ind. Ct. App. 1985) (quoting Globe Indem. Co. v. Daviess, 47 S.W.2d 990, 992 (Ky. 1932)), *reh'g denied*, 484 N.E.2d 617 (Ind. Ct. App.), *and trans. denied*, 484 N.E.2d 617 (Ind. Ct. App. 1986).

20 915 N.E.2d 126 (Ind. 2009).

21 *Id.* at 130 (noting that "[i]t is only slightly more difficult to consider whether the MySpace entry was actually probative of any issue at trial.").

22 Voelker v. Tyndall, 75 N.E.2d 548, 549 (Ind. 1947) ("[T]he [r]ight of [p]rivacy . . . is a well-established doctrine, derived from natural law and guaranteed by both the Federal and [s]tate Constitutions."), *superseded by statute*, Ind. Code § 35-38-5-1 (2010), *as recognized in* Kleiman v. State, 590 N.E.2d 660 (Ind. Ct. App. 1992).

23 *See Retrospective: Ten Key Evidence Issues in 2009*, Fed. Evidence Rev. (Jan. 4, 2010), http://federalevidence.com/blog/2010/january/retrospective-ten-key-evidence-issues-2009 (noting the importance of authenticating evidence, advising juries, and other related issues).

24 *Id.* at n.7 (discussing the Federal Rules of Evidence, which are relevant for states that base their evidence rules off of the federal version).

25 Interview with Jeffrey O. Cooper, Professor, Ind. Univ. School of Law—Indianapolis, in Indianapolis, Ind. (Oct. 29, 2009).

26 Ind. R. Evid. 1002.

27 Ind. R. Evid. 1004.

28 Andrew M. Grossman, Note, *No, Don't IM Me—Instant Messaging, Authentication, and the Best Evidence Rule*, 13 Geo. Mason L. Rev. 1309, 1331 (2006).

29 Ind. R. Evid. 1002; Ind. R. Evid. 1004.

30 Grossman, *supra* note 28, at 1310 (declaring that "the codified authentication and [b]est [e]vidence rule[] provide[s] a reasonable framework for assessing the reliability" of online evidence).

31 *See The Privacy Implications of Cloud Computing*, Privacy Rights Clearinghouse, (Mar. 2009), http://www.privacyrights.org/ar/cloud-computing.htm. The Privacy Rights Clearinghouse is a not-for-profit organization that advocates for privacy rights at the municipal, state, and national level.

32 Camm v. State, 908 N.E.2d 215, 236-37 (Ind. 2009) (finding that controversial demonstrative evidence was admissible because it "appear[ed] to have helped the jury and the court gain a sense of perspective").

33 Richmond Gas Corp. v. Reeves, 302 N.E.2d 795, 800 (Ind. Ct. App. 1973) (citing Evansville Sch. Corp. v. Price, 208 N.E.2d 689 (Ind. Ct. App. 1965)).

34 Ind. R. Evid. 402.

35 *Id.*

36 Ind. R. Evid. 401.

37 Ind. R. Evid. 403.

38 *See generally* Richard A. Posner, *An Economic Approach to the Law of Evidence*, 51 Stan. L. Rev. 1477 (1999).

39 *Id.* at 1543.

40 *See generally* Ind. R. Evid. 404.

41 Ind. R. Evid. 404(a).

42 Ind. R. Evid. 404(b); *see also* Ellen H. Meilaender, Note, *Revisiting Indiana's Rule of Evidence 404(b) and the* Lannan *Decision in Light of Federal Rules of Evidence 413-415*, 75 Ind. L.J. 1103, 1103 (2000) (noting that evidence of other crimes cannot support the general notion of "a propensity to commit crime or a bad character").

43 Cooper, *supra* note 25.

44 Ind. R. Evid. 404(b).

45 *Id.*

46 600 N.E.2d 1334, 1339 (Ind. 1992).

47 *Id.* at 1339-40 (noting that "[w]e are inclined to believe that . . . [this theory] . . . survives our adoption of Rule 404(b)").

48 *Id.* at 1340 (discussing "acts or methods employed" in comparing similar crimes of a given actor).

49 *Id.* (quoting Willis v. State, 374 N.E.2d 520, 522 (Ind. 1978)).

50 *See* Cline v. State, 726 N.E.2d 1249, 1252 (Ind. 2000) (noting that Rule 404(b) is designed to "prevent the jury from making the 'forbidden inference' that prior wrongful conduct suggests present guilt") (quoting Byers v. State, 709 N.E.2d 1024 (Ind. 1999)).

51 795 N.E.2d 1050 (Ind. 2003), *aff'd*, 895 N.E.2d 1201 (Ind. 2008).

52 *Id.* at 1053 (quoting Gibbs v. State, 538 N.E.2d 937 (Ind. 1989)).

53 Fed. R. Evid. 404(b) (emphasis added).

54 Ind. R. Evid. 404(b).

55 Robert Lowell Miller, Jr., 12 Ind. Prac. Series, Indiana Evidence § 404.235 (3d. ed. 2009).

56 *See id.* § 404.203.

57 Hardin v. State, 611 N.E.2d 123, 128-29 (Ind. 2003) (adopting Rule 403 as the prevailing standard for judging evidence and noting that Indiana had moved away from its former "exclusionary rule"), *superseded by statute*, Ind. Code § 35-42-1-1 (2010) (on other grounds), *as recognized in* Swanson v. State, 666 N.E.2d 397 (Ind. 1996).

58 *See* Kubsch v. State, 784 N.E.2d 905 (Ind. 2003), *reh'g denied*, 866 N.E.2d 726 (Ind. 2007).

59 Miller, *supra* note 55, at § 404.235 (3d. ed. 2009) (citing Dickens v. State, 754 N.E.2d 1, 4 (Ind. 2001) (ruling that evidence that the defendant had been seen carrying a gun was relevant and admissible to prove his guilt in a shooting; his "recent act of carrying a gun therefore . . . [went] to opportunity")).

60 *Kubsch*, 784 N.E.2d at 919 (quoting Gilliam v. State, 383 N.E.2d 297, 301 (Ind. 1978)).

61 *See* U.S. v. Green, 648 F.2d 587 (9th Cir. 1981); United States v. McPartlin, 595 F.2d 1321 (7th Cir. 1979)); 22 Wright & Graham, Federal Practice and Procedure: Evidence § 5241 (1978).

62 Ind. R. Evid. 404(b); *cf.* U.S. v. Green, 648 F.2d at 592 n.5 (discussing the Uniform Rules of Evidence and noting that "[t]hough the draftsm[e]n . . . subsequently wrote a manual for practitioners which did not list 'opportunity' among the permissible uses of character evidence[,] it did include the actor's 'ability or capacity to do the wrong.'").

63 U.S. v. Green, 648 F.2d at 592 n.5 (citing 22 Wright & Graham, Federal Practice and Procedure: Evidence § 5241 485 (1978)); United States v. McPartlin, 595 F.2d at 1321.

64 915 N.E.2d 126 (Ind. 2009).

65 *See id.* at 130 (noting that "Clark testified that at most Samantha died because he was drunk and he was 'reckless,'" which arguably goes to his opportunity to have caused her death).

66 Ind. R. Evid. 801(c).

67 Ind. R. Evid. 801(a).

68 Ind. R. Evid. 802.

69 *See* Ind. R. Evid. 801(d); Ind. R. Evid. 803, 804, 805.

70 Ind. R. Evid. 801(d)(2)(A).

71 G. Michael Fenner, The Hearsay Rule 4 n.2 (2009).

72 *See* Mayberry v. State, 670 N.E.2d 1262, 1267 (Ind. 1996) (acknowledging "a valid exception to the rule against hearsay for each level of hearsay"), *reh'g denied*; City of Indianapolis v. Taylor, 707 N.E.2d 1047, 1055 (Ind. Ct. App.) (exploring the intricacies of "double hearsay" in a criminal case), *trans. denied*, 726 N.E.2d 309 (Ind. 1999).

73 *Taylor*, 707 N.E.2d at 1056.

74 Cooper, *supra* note 25.

75 Ind. R. Evid. 901(a) ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.").

76 Ind. R. Evid. 901(b).

77 Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 Cornell L. Rev. 901, 921 (2002).

78 *Id.* (discussing the "divergent incentives of ISPs and their subscribers").

79 Christian C.M. Beams, *The Copyright Dilemma Involving Online Service Providers: Problem Solved . . . for Now*, 51 Fed. Comm. L.J. 823, 830 (1999).

80 Hamdani, *supra* note 77, at 956.

81 St. Clair v. Johnny's Oyster & Shrimp, Inc. 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999) (observing that "[h]ackers can adulterate the content on *any* web-site from *any* location at *any* time"); *see also* David W. Hagy, Nat'l Inst. of Justice, Special Report, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition (2008), *available at* http://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

82 Cooper, *supra* note 25.

83 Hagy, *supra* note 81, at viii.

84 Robert S. Kelner & Gail S. Kelner, *Social Networks and Personal Injury Suits*, N.Y. L.J., Sept. 24, 2009, *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202434026615&Social_Networks_and_Personal_Injury_Suits (last visited Feb. 23, 2011).

85 *Id.* (emphasis added) (citing *St. Clair*, 76 F. Supp. 2d at 775 (in which the court finished that part of the analysis by going so far as to say that "any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed. R. Civ. P. 807.")).

86 J. Shane Givens, *The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards*, 34 Cumb. L. Rev. 95, 106 (2003).

87 Grossman, *supra* note 28, at 1323 (citing 7 John Henry Wigmore, Evidence in Trials at Common Law § 2128 (Chadbourn rev. ed. 1978)).

88 915 N.E.2d 126 (Ind. 2009).

89 Ind. R. Evid. 1002.

90 821 N.E.2d 409, 412 (Ind. Ct. App.), *trans. denied*, 831 N.E.2d 741 (Ind. 2005); Ind. R. Evid. 1002.

91 Ind. R. Evid. 1002.

92 *Id.*

93 Grossman, *supra* note 28, at 1320.

94 Ind. R. Evid. 1002.

95 Ind. R. Evid. 1001(a).

96 903 N.E.2d 977 (Ind. Ct. App.), *trans. denied*, 915 N.E.2d 994 (Ind. 2009).

97 *Id.* at 990 (citing Bone v. State, 771 N.E.2d 710, 716 (Ind. Ct. App. 2002)).

98 Purifoy v. State, 821 N.E.2d 409, 412 (Ind. Ct. App.), *trans. denied*, 831 N.E.2d 741 (Ind. 2005).

99 *See* discussion *supra* Part I.C.

100 *Purifoy*, 821 N.E.2d at 412 (requiring fundamental error to reverse the defendant's conviction).

101 *Id.*

102 915 N.E.2d 126 (Ind. 2009).

103 *Id.*

104 Ind. R. App. P. 4 (A)(1)(a) ("The Supreme Court shall have mandatory and exclusive jurisdiction over . . . [c]riminal [a]ppeals in which a sentence of death or life imprisonment without parole is imposed.").

105 *Clark*, 915 N.E.2d at 127-28.

106 *Id.* at 128.

107 *Id.*

108 *Id.*

109 *Id.* (citing the trial record at 90).

110 *Id.* at 130.

111 *Id.* at 128.

112 *Id.*

113 Privacy Rights Clearinghouse, Fact Sheet 18: Privacy and the Internet: Traveling in Cyberspace Safely, http://www.privacyrights.org/fs/fs18-cyb.htm#Interactive_Use (last visited Mar. 8, 2010) (defining MySpace.com as "an extremely popular Web site that allows people to set up profiles, pictures, and blogs").

114 *Clark*, 915 N.E.2d at 129.

115 *Id.* at 128.

116 Ind. R. Evid. 404(b).

117 *Clark*, 915 N.E.2d at 130 (noting that "Clark's posting contained only statements about himself and in reference to himself").

118 *Id.* at 131.

119 Cooper, *supra* note 25. Professor Cooper is a member of the Committee on Rules of Practice and Procedure.

120 Ind. R. Evid. 404(a) (providing that "evidence of a person's character or a trait of character is not admissible for the purpose of proving action in conformity therewith on a particular occasion" with exceptions for the character of the accused, witnesses, or victims.).

121 Ind. R. Evid. 404(b).

122 *Clark*, 915 N.E.2d at 130.

123 Ind. R. Evid. 404(a)(1).

124 *Id.* (noting that "evidence of a pertinent trait of character offered by an accused, or by the prosecution to rebut the same" is admissible).

125 *Clark*, 915 N.E.2d at 129.

126 *Id.*

127 *Id.* at 130.

128 Ind. R. Evid. 404(a)(1).

129 Black's Law Dictionary (8th ed. 2004).

130 *Clark*, 915 N.E.2d at 128.

131 *Id.* at 129.

132 *Id.* (emphasis added).

133 *See* Ind. R. Evid. 901(b)(1).

134 Monique C.M. Leahy, *Proof of Instant Message, Blog, or Chat as Evidence*, 100 Am. Jur. 3d *Proof of Facts* 89 § 13 (2008) (citing Internet & Email Evidence, SM078 ALI-ABA 247, 255–56 (2007)).

135 *See, e.g.*, A.B. v. State, 885 N.E. 2d 1223 (Ind. 2008).

136 *Id.* at 1223.

137 *Id.*

138 *Id.* at 1224.

139 *Id.* at 1227.

140 *Id.* at 1224.

141 *Id.* at 1227.

142 *Id.*

143 Privacy Rights Clearinghouse, *supra* note 31.

144 *Id.*

145 Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, *Privacy in the Clouds—A White Paper on Privacy and Digital Identity: Implications for the Internet*, *available at* http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf (last visited Mar. 8, 2010).

146 Russ Smith, NTIA Abstract, *The IP Address: Your Internet Identity* (Mar. 29, 1997), *available at* http://www.ntia.doc.gov/ntiahome/privacy/files/smith.htm. The NTIA, or National Telecommunications and Information Administration, is an advisory organization for telecommunications and information policy.

147 Cavoukian, *supra* note 145.

148 *See generally Your Resume May Be Overshadowed by Your Online Persona: Tips for Jobseekers*, Privacy Rights Clearinghouse (July 9, 2006), http://www.privacyrights.org/ar/OnlinePersona.htm (noting that "unlike legitimate background check companies, Web sites do not have a duty to investigate potential errors and correct misinformation").

149 Daniel F. Spulber, *The Map of Commerce: Internet Search, Competition, and the Circular Flow of Information.* 5 J. Competition L. & Econ. 633, 648 (2009).

150 *See generally* Nat'l Inst. of Standards & Tech., http://www.nist.gov/index.html (last visited Feb. 23, 2011). The NIST is a federal technology agency under the supervision of the U.S. Department of Commerce.

151 Nat'l Inst. of Standards & Tech., Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft) § 2-1 (Jan. 2009) (defining personally identifiable information as a category of data ranging "from an individual's name or email address to an individual's financial and medical records or criminal history").

152 *Id.*

153 Nicole Cohen, Note, *Using Instant Messages as Evidence to Convict Criminals in Light of National Security: Issues of Privacy and Authentication*, 32 New Eng. J. on Crim. & Civ. Confinement 313, 335 (2006).

154 381 U.S. 479 (1965).

155 *Id.* at 479, 484.

156 *Id.* at 482-84.

157 *Id.* at 479.

158 Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992).

159 *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890) (discussing evolution of the common law to coincide with this right).

160 Restatement (Second) of Torts § 652B (1965).

161 *Id.* § 652D.

162 *Id.* § 652B.

163 *Id.* § 652D cmt. e.

164 *Id.*

165 *Id.* § 652D cmt. f.

166 *See id.*

167 United States v. Karo, 468 U.S. 705, 726 (1984).

168 Restatement (Second) of Torts § 652D cmt. f (1965).

169 *See* Ian Byrnside, Note, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 Vand. J. Ent. & Tech. L. 445, 452 (2008).

170 *See* U.S. v. Katz, 389 U.S. 347, 361 (1967) (reversing the lower court's decision that recording defendant's public telephone booth conversation did not violate any reasonable expectation of privacy).

171 *Id*.

172 *Id.*

173 Kimberly A. Horn, *Privacy v. Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 Fordham Urb. L. J. 2233, 2265 (2002). *But see* United States v. Maxwell, 45 M.J. 406, 418 (1996) (finding that "the fact that an unauthorized 'hacker' might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way").

174 *Id.* at 2265-66.

175 *See* discussion *supra* Part III.A.

176 *See* Restatement (Second) of Torts § 652D cmt. e (1965).

177 *See id.*

178 767 N.W.2d 34 (Minn. Ct. App. 2009).

179 *Id.* at 43 (finding that postings on social networking sites need not appeal to the "general interest" like a newspaper to be considered "publicity").

180 Laura Saunders, *Is "Friending" in Your Future? Better Pay Your Taxes First*, Wall St. J., Aug. 27, 2009, at A2, *available at* http://online.wsj.com/article/SB125132627009861985.html ("State revenue agents have begun nabbing scofflaws by mining information posted on social-networking Web sites, from relocation announcements to professional profiles to financial boasts.").

181 *Id.*

182 *Id.* (noting that "agents are not allowed to 'friend' someone using false information"); *see also* Karen Setze, *State Tax Officials Using Clues from Social Networking Sites*, Tax.com: Featured Articles (Aug. 2009), http://www.tax.com/taxcom/features.nsf/Articles/57E3F85755CBB802852576190049753C (noting that Nebraska agents made use of the networking sites after being led there by a public search engine).

183 Pete Thomas, *Wisconsin Authorities Visit Facebook to Find Evidence of Illegal Deer Hunting*, L.A. Times, Sept. 10, 2009, *available at* http://latimesblogs.latimes.com/outposts/2009/09/wisconsin-authorities-visit-facebook-to-find-evidence-of-illegal-deer-hunting-.html; Mike Johnson,

Facebook Video Leads to Deer Shining Charges, Milwaukee J. Sentinel, Sept. 8, 2009, *available at* http://www.jsonline.com/news/waukesha/57810647.html.

184 Johnson, *supra* note 183.

185 Thomas, *supra* note 183 (noting that Frame also posted the comment "I just posted a video from us hunting at 4 a.m. drunk in a subdivision with my headlight lighting it up" on Facebook).

186 State v. Frame, No. 2009CM000956 (Waukesha Cnty. filed Apr. 23, 2009, decided Aug. 2009); State v. Porter, No. 2009CM001841 (Waukesha Cnty. filed Aug. 24, 2009); Thomas, *supra* note 184.

187 *See* Saul Hansell, *Government 2.0 Meets Catch 22*, N.Y. Times (Mar. 17, 2009), http://bits.blogs.nytimes.com/2009/03/17/government-20-meets-catch-22.

188 *See* Blogs from the U.S. Gov't, http://www.usa.gov/Topics/Reference_Shelf/News/blog.shtml (last visited Mar. 8, 2010).

189 *See* Hansell, *supra* note 187.

190 *See generally Computers & the Internet: Privacy & Security*, Fed. Trade Comm'n, http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm (last visited Jan. 17, 2010).

191 Fed. Trade Comm'n, Privacy Online: A Report to Congress 3 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (reporting that "in early 1997, 51 million adults were already online in the U.S. and Canada, and . . . [b]y December 1997, the number of adults online in the U.S. and Canada had climbed to 58 million") [hereinafter FTC, Privacy Online].

192 *See generally id.*

193 *See* Dorothy A. Hertzel, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 Fed. Comm. L.J. 429, 433 (2000) (citing Fed. Trade Comm'n, *supra* note 191, at 19.

194 Fed. Trade Comm'n, *supra* note 191 at 10 n.53 (reporting that the European Union "has recognized that self-regulation may in certain circumstances constitute 'adequate' privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking 'adequate' safeguards).

195 *See generally* Fed. Trade Comm'n, Online Profiling : A Report To Congress, Pt. 2: Recommendations (2000); Fed. Trade Comm'n, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last updated June 25, 2007) (adding the fifth core principle to the existing set of four) [hereinafter FTC, Fair Info.].

196 FTC, Fair Info., *supra* note 195.

197 *See generally id.*

198 *Id.* at 20.

199 *Id.* (emphasis added).

200 *Id.* (emphasis added).

201 *Id.* (emphasis added).

202 *Id.*

203 *Id.*

204 *See generally* Fed. Trade Comm'n, Staff Report, Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology (2009).

205 *Id.* at 37-41.

206 *Id.* at 46.

207 *Id.*

208 *Id.*

209 Proposed Revision of the Policy on Web Tracking Technologies for Federal Websites, Notice of Call for Comments, 74 Fed. Reg. 37062-01 (July 27, 2009).

210 *Id.* at 37063.

211 *Id.*

212 *Id.*

213 *Id.*

214 *Id.*

215 Godwin et al., Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions (Dec. 23, 2008), *available at* http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf.

216 *Id.*

217 *Id.*

218 Congressman Rick Boucher, Communication Networks and Consumer Privacy: Recent Developments: Statement Before the Subcommittee on Communications, Technology and the Internet (Apr. 23, 2009).

219 *Id.*

220 *See generally* 15 U.S.C. §§ 6501-06 (2006).

221 *See generally* 44 U.S.C. § 3501 (208) (2006).

222 Kathryn Montgomery & Shelley Pasnik, *Responsible Advertising to Children and Youth in the New Online Environment* (Apr. 21-25, 2007) (presented at the Forum International de Chercheurs "Les Jeunes et les Médias, Demain" at the United Nations Educational, Scientific, and Cultural Organization Conference in Paris).

223 Danielle J. Garber, Note & Comment, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & Pol'y 129, 139-40 (2001) (citing FTC, Privacy Online, *supra* note 191).

224 15 U.S.C. § 6502(D) (2006) (the entire Children's Online Protection Privacy Act is codified at *id.* §§ 6501-06).

225 *See* Prince v. Massachusetts, 321 U.S. 158, 169 (1944) (noting that with respect to the "evils of the streets" and their effect on children, "what may be wholly permissible for adults therefore may not be so for children, either with or without their parents' presence").

226 44 U.S.C. § 3501 (208)(b)(1)(B)(iii) (2006) (codifying the Electronic Government Act of 2002).

227 Memorandum from the Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22) (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda_m03-22/.

228 44 U.S.C. § 3501 (208)(b)(2)(B)(i)-(vii) (codifying the Electronic Government Act of 2002).

229 *See* United States v. Meek, 366 F.3d 705, 711 (9th Cir. 2004); United States v. Maxwell, 45 M.J. 406, 418 (1996); Commonwealth v. Proetto, 771 A.2d 823, 829-830 (Pa. Super. Ct. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003).

230 *See generally* 44 U.S.C. § 3501 (208)(b)(1)-(3).

231 Google Privacy Ctr., Privacy Policy, Mar. 11, 2009, http://www.google.com/privacypolicy.html (last visited Mar. 8, 2010).

232 *Id.*

233 MySpace Privacy Policy, Feb. 28, 2008, http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last visited Mar. 8, 2010).

234 *Id.*

235 *Id.*

236 *See Online Personal Privacy Act: Hearing on S. 2201 Before the Committee on Commerce, Science, and Transportation*, 107th Cong. 2 (2002) (statement of Marc Rotenberg, Executive Director, Elec. Privacy Info. Ctr.).

237 *Id.*

238 *Id.*

239 *Id.*

240 President Barack Obama, Remarks by the President in Discussion with Ninth Graders at Wakefield High School (Sept. 8, 2009), *available at* http://www.reuters.com/article/idUSTRE58762P20090908?feedType=RSS&feedName=internetNews.

241 Byrnside, *supra* note 169, at 461 (citing Martha Irvine, *When MySpace Becomes Everyone's Space*, Globe & Mail (Toronto), Dec. 30, 2006, at R12).

242 Ind. R. Evid. 801(a).

243 *Id.*

244 Brad Stone & Brian Stelter, *Facebook Withdraws Changes in Data Use*, N.Y. Times, Feb. 19, 2009, at B1, *available at* http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html (noting that "Facebook has been redefining notions of privacy while growing so rapidly that it now has 175 million active users, giving it a population larger than most countries").

245 Facebook's Privacy Policy, Dec. 9, 2009, http://www.facebook.com/policy.php?ref=pf (last visited Mar. 8, 2010) (emphasis added).

246 Ind. R. Evid. 901(b)(10).

247 *See* Ind. R. Evid. 902.

248 *See* Facebook Press Room, Facebook Announces Privacy Improvements in Response to Recommendations by Canadian Privacy Commissioner (Aug. 27, 2009), http://www.facebook.com/press/releases.php?p=118816.

249 An Act to Establish Rules of Evidence for Certain Courts and Proceedings, Pub. L. No. 93-595 (January 2, 1975) (establishing the Federal Rules of Evidence); Stephen C. Bower, *Relevancy: Old Rule, New Approach*, 38-Jul Res Gestae 18, 18 (1994) (noting that the Indiana Rules of Evidence took effect Jan. 1, 1994).

250 Bower, *supra* note 249, at 23.

251 578 N.E.2d 649 (Ind. 1991).

252 *Id.* at 652 (noting that in 1975, most jurisdictions in the United States "prohibited admission of prior statements of any nature for any purpose other than impeachment").

253 *Id.*

254 Ind. R. Evid. 102.

255 Fed. R. Evid. 102 ("These rules shall be construed to secure fairness in administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained and proceedings justly determined.").

256 Huff v. White Motor Corp., 609 F.2d 286, 295 (7th Cir. 1979).

257 903 N.E.2d 977 (Ind. Ct. App.), *trans. denied*, 915 N.E.2d 994 (Ind. 2009).

258 *Id.* at 984.

259 *Id.*

260 *Id.* at 998 (citing the trial record at 320).

261 *Id.* at 991 (citing Stephenson v. State, 742 N.E.2d 463, 477 (Ind. 2001)).

262 *Id.* at 986.

263 *Id.* at 988 (quoting Black's Law Dictionary 842 (8th ed. 2004)).

264 *Id.*

265 *Id.* at 991.

266 Fed. R. Evid. 901(b)(1) ("Testimony of witness with knowledge . . . that a matter is what it is claimed to be").

267 Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007).

268 United States v. Kassimu, 188 Fed. Appx. 264, 265 (5th Cir. 2006) (ruling that an "otherwise qualified witness" with comprehensive knowledge of the technology could authenticate electronic post office records).

269 235 F.3d 1318, 1322-23 (11th Cir.2000).

270 Fed. R. Evid. 901(b)(4).

271 *Lorraine*, 241 F.R.D. at 546.

272 *Id.* at 548 (citing U.S. Dist. Ct. for the Dist. of Md., Suggested Protocol for Discovery of Electronically Stored Information ("ESI"), *available at* http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (last visited Jan. 18, 2010)).

273 *Id.* "Hash values" are similar to identifying numbers that are commonly placed on paper documents.

274 U.S. Dist. Ct. for the Dist. of Md., *supra* note 272, at 20.

275 Warren & Brandeis, *supra* note 159, at 193.

276 *Id.* at 194 (calling for the law to secure "what Judge Cooley calls the right 'to be let alone'").

277 McMann v. Doe, 460 F. Supp. 2d 259, 266 (D. Mass. 2006).

278 *Id.* at 259.

279 *Id.* at 266.

280 Donald Carrington Davis, Note, *MySpace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services*, 16 Kan. J. L. & Pub. Pol'y 237, 239 (2007).

281 *Id.*

Job Search Assistance!

Susanna Brennan, Recruitment Director for Kelly Law Registry, and Council Member for the Information Technology Section of the State Bar of Michigan, is available to assist Section Members with resume feedback, interviewing tips, and job search assistance. Susanna is an experienced recruiter and career consultant who places attorneys and legal professionals in contract and permanent positions with law firms, corporate legal departments, and other organizations in the Midwest. For more information, please contact Susanna at *brennsc@kellylawregistry.com* or (248) 952-0539. ■

Publicly Available Websites for IT Lawyers

Following are some publicly available websites relating to varying aspects of information technology law practice. Some of these websites may require payment for certain services. Neither the State Bar of Michigan nor the IT Law Section endorses these websites, the providers of the website, or the goods or services offered in connection therewith. Rather these websites are provided for information purposes only and as possible useful tools for your law practice.

Please provide any feedback or recommendations for additional websites to *michael@gallo.us.com*.

Security

- *http://keepass.info* – 'KeePass Password Safe', a free, open-source light-weight and easy to use password manager
- *http://www.truecrypt.org* – 'TrueCrypt' is a free, open-source disk encryption application.
- *http://secunia.com/products/consumer* - Secunia offers software inspection tools that scan a personal computer and secure it against vulnerabilities in commonly used Windows programs
- *http://www.microsoft.com/security_essentials* - Microsoft Security Essentials provides free, real-time protection for computers

2011 Edward F. Langs Writing Award

Essay Competition Rules

1. Awards will be given to up to three 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 $1,500 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*.
7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2011, and emailed to ***dsyrowik@brookskushman.com***. ■