# NFJE Looks at Technological Advances and Their Effect on the Law at Seventh Annual Symposium

By Michelle Parrini

The National Foundation for Judicial Excellence (NFJE) sponsored its seventh annual judicial symposium, "Applied Science and the Law: 21st Century Technology in the Courts," July 15–16, 2011, in Chicago at the Swissôtel with great success. Attended by 129 state court judges and justices from 35 states, the symposium delved into how exponential technological growth and the consequential increase in the ability to process information will affect and has affected the law and judicial practice by examining five topics important to courts: written advocacy in a paperless world, social media's role in the law, Internet data breaches and the law, human biomonitoring and genetic biomarker technologies' intersection with traditional tort law concepts, and electronic communication privacy rights in workplaces.

The symposium opened on Friday, July 15, 2011, with a presentation by Robert B. Dubose, a partner with Alexander Dubose & Townsend LLP practicing from Houston. Setting the scene for his topic, Mr. Dubose said that his talk would "follow the theme of classic Science Fiction, that technology doesn't just do things for us, it does things to us." Specifically, as we have switched from reading on paper to reading on screens, the technology that we use has changed us.

According to Mr. Dubose, screen reading differs fundamentally from paper reading in several ways with implications for brief writing, brief formatting, and law practice. *See also* Robert B. Dubose, *Legal Writing for the Rewired Brain: Communication in a Paperless World* 5–18 (NFJE 2011) (discussing the current reading environment and its effects on legal practice and proposing changes to briefs), http://www.nfje.net/Programs.aspx?event=2011AJS (follow "Course Materials" hyperlink). For instance, search engines such as Google require little thought to use, so researchers expect quick answers and to find them easily. This, Mr. Dubose pointed out, has changed legal research. To illustrate that point, he showed the audience a PowerPoint slide capturing a West Law electronic database screen highlighting in yellow the word "appraisal." Rather than a paper digest, which requires understanding broad legal principles and the "map of the law" in a digest's table of contents, new legal researchers today use search engines that require choosing and inputting a few words describing issues. They can then mistakenly think that they have found "the" law. *See also id.* at 8–10 (describing the screen-reading environment).

This screen-reading environment, Mr. Dubose argued, has changed the way that we read and process information, promoting very different reading from the "deep reading" that we have practiced for hundreds of years. "Deep reading" basically means "going beyond the text to analyze, infer and think new thoughts." Maryanne Wolf, *Our Deep Reading Brain: Its Digital Evolution Poses Questions*, Neiman Reports Online Exclusive (Neiman Found. for Journalism, Harvard Univ. Summer 2010) (last visited Aug. 4, 2011). The readers who have emerged from screen reading do not read deeply. *See also id.* at 10–13 (discussing screen-reading characteristics). Screen readers don't read word for word in a linear way; they jump around a screen, searching for information, "defying" writers' expectations. Screen readers want information quickly and easily, and they have little patience when they don't get it. He and others have noticed a new, "cultural," short attention span. Mr. Dubose surmised that lawyers won't be immune, although he expressed that most legal reading today fuses screen-reading traits with deep-reading traits. Finally, just as online texts have adapted to screen-reading characteristics, Mr. Dubose proposed that the brief adapt. He proposed that the brief: (1) change format, becoming a series of linked, short texts, for instance by using bookmarking or similar functions, to offer readers a way to understand a document's logic quickly, and perhaps change to horizontal page layouts; (2) enable skimming with headings, paragraph topic sentences, visible outlines, lists, and bullets—"structural cues"; (3) arrange texts in "chunks," meaning break complex information into digestible parts, because readers process information in chunks; (4) use more white space because studies indicate that it makes text easier to read; and (5) "make it simple," editing heavily and omitting extra words. *See also id.* at 14–18 (outlining adapting briefs to new realities). Commenting on Mr. Dubose's presentation, one symposium participant said, "It forced me to reflect on my own reading habits as well as anticipate the upcoming changes in briefing."

The Saturday, July 16, events opened with Marisa Trasatti, a principal with Semmes Bowen & Semmes in Baltimore, and the Honorable Michele D. Hotten of the Court of Special Appeals for the Fourth Appellate Circuit, Prince George's County, Maryland. They addressed social media's role in the law, which, given social networking-use trends, will probably continue to grow, and how social media affects the courts. According to one source, Silicon Alley Insider, information sharing through Facebook has now eclipsed sharing through e-mail. In addition to leading to new law, social media increasingly has affected judicial conduct, discovery, evidence authentication, jury selection, and jury misconduct issues, each of which Ms. Trasatti and Judge Hotten discussed. *See also* Marisa Trasatti & Hon. Michele Hotten, *Understanding the Role of Social Media in the Law* 21 (NFJE 2011) (providing hyperlinks to articles and opinions on these topics), *see* Dubose, *supra*, for symposium course material URL. For example, Judge Hotten explained a December 2010 opinion discussing whether the Ohio Code of Judicial Conduct permitted a judge to befriend a lawyer who appears before that judge in a case on a social networking site. Bd. of Comm'r on Grievances and Discipline, Sup. Ct. of Ohio, Op. 2010-7 (2010); *see also* Trasatti & Hot-

ten, *supra*, at tab 39 (hyper-linking to the opinion). In Ohio, a judge may befriend an attorney on social networking sites who appears before that judge in a case as long as the judge upholds the judicial canons and Ohio judicial conduct rules, which the board of commissioners acknowledged "may be challenging for a social networking judge." *Id.* The opinion counseled social networking judges to exercise care mindfully and vigilantly to comply with the rules of conduct when engaged in social networking sites, Judge Hotten explained.

When the discussion turned to evidence authentication, the speakers mentioned *Griffin v. State of Maryland*, 19 A.3d 415 (Md. Apr. 28, 2011); *see also* Trasatti & Hotten, *supra*, at tab 24 (hyper-linking to the opinion). In that case the petitioner, Griffin, appealed his murder conviction partly on the grounds that the trial judge had abused his discretion in admitting as evidence pages printed from Griffin's girlfriend's MySpace profile without proper authentication. The majority held that the pages had not been properly authenticated, reversed the court of special appeals' judgment, and remanded the case. Two of the judges who decided that case, the Honorable Lynne A. Battaglia, who wrote the majority opinion, and the Honorable Glenn T. Harrell, who wrote a dissent joined by another judge, sat in the audience and graciously elaborated on their legal positions. Apparently Mr. Griffin's girlfriend testified during the trial but was never asked if she wrote the disputed MySpace posts, Judge Battaglia explained. The majority noted that anyone could create an account under an alias or access another's account after obtaining the account holder's username and password. Judge Harrell explained that the dissenters thought that Maryland's evidence authentication rule, modeled on Fed. R. Evid. 901, established a low hurdle.

Next up Christopher Day, senior vice president, secure information services of Terremark Worldwide, Inc., in Miami, Florida, and Michele A. Whitham, a partner of Foley Hoag LLP in Boston, discussed data breaches, how they happen technologically, and the legal responses. Mr. Day described who breaches data, from the least to most harmful bad actors, introducing symposium participants to a whole new vocabulary, such as "script kiddies," the "least dangerous" bad actors, and what motivates the worst bad actors, namely, the black market for trading stolen information. He explained some high-profile data-breach cases, such as the one that shut down the Sony Play Station Network and cost the company $170 million in the 2011 fiscal year. Then Mr. Day described how a breach actually happens mechanically, sketching one breach category, an "APT," or "advanced persistent threat," often associated with nation-state and organized crime activity. Mr. Day closed by outlining some grand-scale solutions to the problems associated with data breaches. In particular, Mr. Day recommended partnering with other nations' local law enforcement and changing federal laws to increase the currently very small penalties.

Afterward Ms. Whitham explained the legal responses to data breaches. On the federal level, Congress has regulated data breaches by subject matter and has delegated enforcement by private rights of action to specific agencies. State statutes have required entities to follow rules to keep private data private and to notify individuals when data breaches occur. *See also* Christopher Day & Michele A. Whitham, *Anatomy of Data Breaches: The Technology of How They Happen and the Legal Response* 31–67 (NFJE 2011) (describing the federal and state statutes governing data breaches, legal hurdles, exemplary cases, and emerging appellate law issues), *see* Dubose, *supra*, for URL. Ms. Whitham led symposium attendees through three civil data breach scenarios, "the thieving employee, the corporate competitor, and the hacker for profit," describing typical bad actor profiles, how companies typically discover breaches, the general legal responses, and appellate issues. For instance, a "thieving employee" case usually requires a federal district court to interpret the Computer Fraud and Abuse Act, 18 U.S.C. §1030, specifically, to define "without authorization" and interpret "exceeded authorized access." *See also id.* at 40 (elaborating). The "consumer" as opposed to the financial track of hacker-for-profit cases regularly ask appellate courts to answer, "What constitutes legally cognizable harm to confer standing?" Often consumer cases plead risks of identity theft, but some courts find that too remote to constitute harm. *See also id.* at 39 (elaborating). Other courts have found that plaintiffs had standing, but they dismissed the claims because state law did not establish compensable damages or the plaintiffs failed to plead damages sufficiently. *See also id.* at 38–39 (explaining specific cases on point). Ms. Whitham remarked that two recent California federal court decisions "may indicate a new direction" based on the ideas that "personal information constituted valuable property," the company to which it was provided promised to safeguard it, and the "property interest" could support standing. *See also id.* at 39–40 (discussing the Cal. cases). Ms. Whitham closed by predicting that attorneys would file more class actions, and the United States eventually would regulate and federalize the web, as in India, which made "intermediaries" responsible for patrolling the web. Amol Sharma, *Digerati See Censorship in New Web Rules*, India Real Time, Wall Street J., May 2, 2011, http://blogs.wsj.com/indiarealtime/2011/05/02/digerati-see-censorship-in-new-web-rules/ (last visited Aug. 8, 2011).

During the following session, Professor Gary E. Marchant, the Lincoln Professor of Emerging Technology, Law & Ethics of the Sandra Day O'Connor College of Law, Arizona State University, and Bernard Taylor, Sr., a partner of Alston & Bird LLP practicing from Atlanta, explained how human biomonitoring and genetic biomarkers have intersected with tort law, and as the science advances, may influence it in the future. Dr. Marchant focused on biomarkers of exposure and their effect in litigation, focusing on exposure, proving causation, and potential new causes of action, while Mr. Taylor focused on biomarkers of susceptibility in litigation. "Biomarkers can help both plaintiffs and defendants, depending on the cases, just as DNA has," Dr. Marchant said. *See also* Gary E. Marchant & Carson Schmidt, *Understanding Tort Law Impacts Created by Scientific Advances of Human Biomonitoring and Genetic Biomarkers* 149–168 (NFJE 2011) (explaining types of biomarkers of exposure and of effect and biomonitoring, their applications in litigation and in particular cases, legal obstacles, and complications), *see* Dubose, *supra*, for URL. Generally, scientists classify biomarkers into "three broad categories measuring" exposure, effect, or

susceptibility in individuals. *Id.* at 151. Biomarkers identify subcellular and molecular changes. Biomonitoring, on the other hand, measures "levels of the toxic substance itself or its metabolites in the body." *Id.* at 151. It is often used to demonstrate exposure or its absence in toxic tort cases. Dr. Marchant predicted that biomarker evidence will "proliferate" in litigation, and he wondered if courts will eventually require offering them as evidence to prove exposure. *See also id.* at 154–57 (discussing the technologies as evidence in specific court cases to demonstrate exposure).

The key issues that these technologies raise are premature or invalid use, pressure to expand the scope of liability, and ethical. "Most scientists think that this technology is not quite ready to verify tort liability, but it will be," Dr. Marchant said. And when that happens, biomarkers may, for instance, help prove specific causation if a particular plaintiff can demonstrate that he or she has an agent- or chemical-specific biomarker of effect, while the reverse would benefit a defendant. *See also id.* at 157–60 (discussing the technologies as introduced in specific court to prove causation). Courts already have admitted this kind of evidence, Dr. Marchant said, citing as an example *Tompkin v. American Tobacco*, 2001 WL 36112663 (N.D. Ohio 2001). And although the courts haven't supported latent injury claims generally, biomarkers and biomonitoring evidence may in the future support them. *See also id.* at 161–63 (elaborating). Additionally, when the science matures, it may support a new cause of action, "toxic trespass," which posits that an unwanted foreign substance in someone's body invades the personal property of the body, and as with real property trespass, wouldn't require establishing a present injury. *See also id.* at 163–64 (discussing toxic trespass).

Dr. Marchant concluded by posing questions that the law and policy makers will need to confront as science advances. Will accepting latent disease claims open litigation floodgates? How will courts validate biomarker evidence before admitting it? Can juries comprehend biomarker and biomonitoring evidence? When will we compensate people? And how will we protect plaintiffs' privacy and shield them from discrimination, since defendants may seek biomarker data to disprove claims just as plaintiffs may seek to introduce it as evidence?

Speakers at the symposium (from left): the Hon. Michele D. Hotten, Kent L. Richland, Deborah L. Whitworth, Christopher Day, Michele A. Whitham, Bernard Taylor, Sr., Gary E. Marchant, Marisa Trasatti and Lewis Maltby.

Mr. Taylor explained applying genetic susceptibility data in toxic tort litigation to causation, duty to warn, class certification, and damages. "We need to make decisions that reach the right results for plaintiffs," he began. Plaintiffs have difficulty satisfying the "more likely than not" causation standard, which requires a plaintiff to demonstrate that a defendant's actions doubled the plaintiff's relative risk of developing an illness. In some cases a plaintiff with genetic susceptibility to developing a disease could use testing to support causation arguments, perhaps even diminishing that "doubling the risk" threshold. *See also* Bernard Taylor Sr. & Eric D. Gardner, *Evidence of Genetic Susceptibility in Toxic Tort Litigation* 173 (NFJE 2011) (discussing relevant cases), *see* Dubose, *supra*, for URL. On the other hand, testing could harm a plaintiff's case if that plaintiff's test results reveal that he or she did not have genetic susceptibility when the plaintiff's attorney argued that genetic susceptibility in some people increases a risk associated with a product, as happened in *Easter v. Aventis Pasteur Inc.*, 358 F. Supp 2.d 574 (E.D. Tex. 2005). And a defense attorney, Mr. Taylor explained, could use genetic susceptibility data to support an alternative causation argument that a disease resulted from a genetic predisposition rather than a product. *See also id.* at 174 (discussing cases on point). "Plaintiffs will need to agree or we will need to decide if plaintiffs must have DNA tests to support claims," Mr. Taylor remarked, which will lead to privacy objections as more defense attorneys seek genetic susceptibility data from unwilling plaintiffs. "We will also need to decide," Mr. Taylor said, "if we should hold a nonnegligent manufacturer liable for failing to warn a few hypersensitive individuals that a product can injure them." Most cases have found that manufacturers have a duty to test but not to withhold a product because it may harm certain hypersensitive individuals. *See also id.* at 175 (elaborating).

As for class certification, arguing that determining risk and causation requires evaluating individual differences in the genetic predisposition to risk among potential class members could defeat class certification in some instances. *See also id.* at 175 (citing cases). And defense attorneys have argued that courts should adjust damage awards due to preexisting conditions, so a defense attorney may argue that a plaintiff's genetic susceptibility to a disease should alter calculating damages. *See also id.* at 175 (citing preexisting conditions damages issues cases). One symposium attendee asked, "When would a court appropriately order discovery of genetic testing when it already exists, and when would a court appropriately order a test if it didn't exist?" Although guidelines don't exist yet, both speakers agreed that ordering a test or its production would require a plausible scientific reason to prevent "a fishing expedition."

After lunch, three individuals spoke on employers' right to access employees' electronic communications and employee Fourth Amendment privacy rights: Kent L. Richland, a founding partner of Greines Martin Stein & Richland LLP in Los Angeles, Lewis Maltby, president of the National Workrights Institute in Princeton, New Jersey, and Deborah L. Whitworth, director of human resources consulting with Lebel

& Harriman LLP in Falmouth, Maine. Mr. Richland successfully represented the city in the U.S. Supreme Court in *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), much anticipated as the first Supreme Court case to consider privacy rights in digital communications, specifically, employer-provided, portable, text-message enabled pagers. Grounding the opinion in the plurality approach in *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Court held that the city police department conducted a reasonable search of a SWAT team member's employer-provided pager in reviewing test messages sent through it to determine if the city's text message plan allotment sufficed for work purposes, unanimously reversing the Ninth Circuit decision. But the Court declined to determine if the *O'Connor* plurality approach or Justice Scalia's alternative approach in *O'Connor* governed because the petitioners and respondents agreed that it did, as well as whether the employee, Quon, had a reasonable expectation of privacy. Nor did it resolve whether the search violated the rights of individuals who sent text messages to Quon. *See also* Kent L. Richland, *City of Ontario V. Quon: Evolution of a Narrowly Decided Landmark* 133–34, 136 (NFJE 2011) (discussing *Quon*), *see* Dubose, *supra*, for URL.

Mr. Richland described the unusual circumstances that led, in his view, to a narrow opinion. First, some amicus briefs "urged caution" in applying the Fourth Amendment to new, evolving communication technologies, partly because fluid workplace communication standards didn't offer a sound foundation for determining reasonableness. *See also id.* at 135 (discussing the briefs). Second, the oral argument, which Mr. Richland characterized as "entertaining" and "unsettling," seemed to indicate that some justices were themselves "mystified" by digital technology and unprepared to issue an expansive ruling. *See also id.* at 135 (describing the oral argument). Third, it seemed that blog commentary influenced the decision, particularly Orrin Kerr's commentary. Kerr, a recognized law and digital media expert, had clerked for Justice Kennedy, who wrote the *Quon* opinion. For instance, after the oral argument, Kerr wrote that the courts aren't set up to deal with technology in flux; that responsibility belonged with the legislature. *See also id.* at 135–36 (describing Kerr's commentary in detail). Fourth, the Court assumed that a reasonable expectation of privacy existed rather than deciding whether it did, which as an attorney, Mr. Richland found illogical.

Commenting on *Quon*'s significance, Mr. Richland predicted that it would influence other opinions despite its narrow frame: 29 cases, he said, already have cited it, and one Sixth Circuit opinion mentioned that *Quon* at least implies that employees have a reasonable expectation of privacy in the workplace both in public and private settings. Additionally, Mr. Richland mentioned that readers have interpreted the opinion as endorsing the idea that the Constitution's meaning changes over time, pointing out that Professor Liu indicated as much during his confirmation hearing for a seat on the Ninth Circuit. Finally, blogs probably did have some effect, which may augur the future. The opinion authored by Justice Kennedy appeared closely aligned with Kerr's commentary. And "Justice Scalia has admitted," Mr. Richland said, "that his clerks read blogs."

In contrast, Mr. Maltby interpreted "*Quon* as deciding that employees do not have an expectation of privacy and that employer policy trumps everything." In Mr. Maltby's opinion, the Court didn't apply a reasonable expectation test or a reasonable man test. He viewed the test as "an ownership test." In *Quon*, the employer's policy reserved the right to monitor employee communications on employer-issued devices, and even though Quon's immediate supervisor said that he wouldn't monitor, and the employer generally did not monitor communications, Quon still did not have a reasonable expectation of privacy. In Mr. Maltby's view, courts generally have applied "an ownership test" to determine reasonable expectations of privacy: a reasonable expectation of employee privacy existed depending on whether the employee or the employer "owned the system through which" communication happened. *See also* Lewis Maltby, *Employment Privacy: Time for New Paradigm* 143–44 (NFJE 2011) (discussing other cases), *see* Dubose, *supra*, for URL. "We don't live in a world where the employer owns the computer or network" in every instance anymore, he noted. Third parties own networks, and employees own many technologies that they use for work. The search in *Quon* violated the Stored Communication Act, Mr. Maltby continued, which requires device issuers to receive consent from recipients of communications sent through those devices before the issuers can view them. In Mr. Maltby's opinion, under the "ownership paradigm," no one receives fair treatment. Even if an employer has reason to view electronic communications, the employer would only have that a right if it owned the communication device. He proposed adopting a "legitimate interest paradigm" to create fairness given today's work realities, which would permit an employer access to information "based on legitimate interest, not based on ownership."

Finally Ms. Whitworth counseled that employers set expectations, communicate them regularly, and then enforce them, adding that because the boundary between work and personal life increasingly has become blurry, she personally didn't know of any employers enforcing zero tolerance policies on using company-owned devices for personal use. She also described best practices, which boil down to creating and distributing (1) acceptable use policies; (2) discipline policies; (3) and search policies. *See also* Deborah L. Whitworth, *Employer-Owned Portable Electronic Equipment and Employee-Generated Electronic Communications: What Is an Employer to Do?* 71 (NFJE 2011) (describing developing policies and using best practices and providing policy examples), *see* Dubose, *supra*, for URL.

The symposium wrapped up with a lively question and answer moderated by Dan D. Kohane, a senior member of Hurwitz & Fine PC in Buffalo, New York, which permitted symposium attendees to address all the speakers before everyone adjourned to the Swissôtel's 43rd floor for an event-concluding reception. Topics ran the gamut from whether an appellate panel may bring in an expert panel to inform decision making, to using protective orders to maintain privacy when courts compel plaintiffs to have DNA tests, to whether dead people have DNA privacy rights. To quote one symposium participant, "The faculty was articulate, well versed, and current on their topics and made for a dynamic and cutting-edge program. Well done!"