January/February 2009

Boston Bar Journal

A Publication of the Boston Bar Association

Web 2.0 and the Lost Generation

Web 2.0: What's Evidence Between "Friends"?

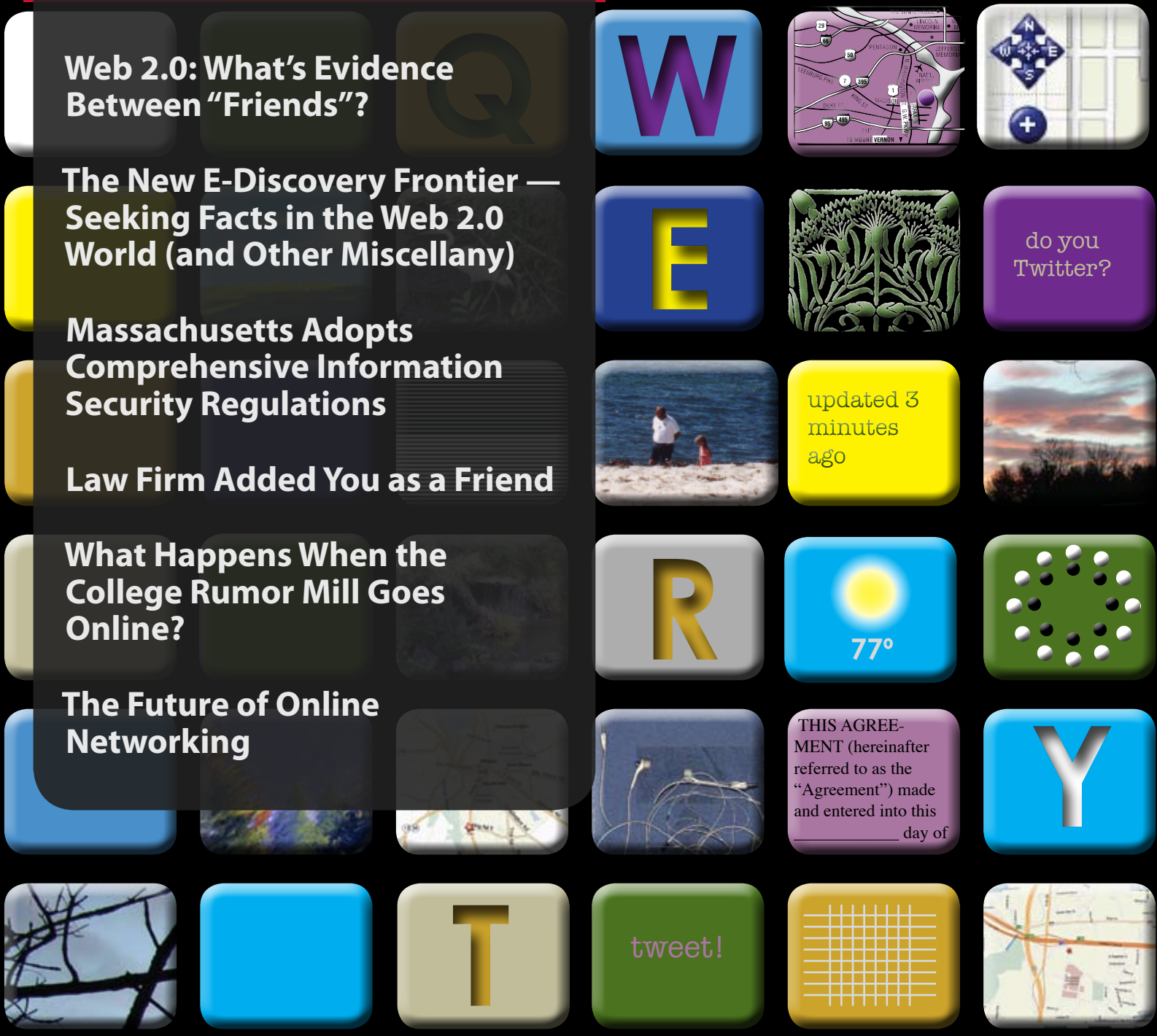
The New E-Discovery Frontier — Seeking Facts in the Web 2.0 World (and Other Miscellany)

Massachusetts Adopts Comprehensive Information Security Regulations

Law Firm Added You as a Friend

What Happens When the College Rumor Mill Goes Online?

The Future of Online Networking



GROW YOUR 401(k) WISELY

ABA Retirement Funds™



Six things you won't hear from other 401(k) providers...

1. We were created as a not-for-profit entity, and we exist to provide a benefit
2. We leverage the buying power of the ABA to eliminate firm expenses and minimize participant expenses
3. Our fiduciary tools help you manage your liabilities and save valuable time
4. Our investment menu has three tiers to provide options for any type of investor, and our average expense is well below the industry average for mutual funds
5. We eliminated commissions, which erode your savings, by eliminating brokers
6. We have benefit relationships with 29 state bar and 2 national legal associations.* No other provider has more than one.

LEARN HOW YOU CAN GROW YOUR 401(k) WISELY

Call an ABA Retirement Funds Consultant at

1-877-947-2272

www.abaretirement.com

* Alabama State Bar
State Bar of Arizona
Arkansas Bar Association
Colorado Bar Association
Connecticut Bar Association
The District of Columbia Bar
State Bar of Georgia
Hawaii State Bar Association
Illinois State Bar Association
Indiana State Bar Association
Iowa State Bar Association
Kansas Bar Association
Louisiana State Bar Association
Maine State Bar Association
Minnesota State Bar Association
The Mississippi Bar
State Bar of Nevada
New Hampshire Bar Association
State Bar of New Mexico
New York State Bar Association
North Carolina Bar Association
State Bar Association of North Dakota
Ohio State Bar Association
Oklahoma Bar Association
Rhode Island Bar Association
State Bar of Texas
Vermont Bar Association
Washington State Bar Association
State Bar of Wisconsin
American Immigration Lawyers Association (AILA)
Association of Legal Administrators (ALA)

ABA Defending Liberty Pursuing Justice

ABA Member Advantage The Buying Power of Your Membership

For a copy of the Prospectus with more complete information, including charges and expenses associated with the Program, or to speak to a Program consultant, call 1-877-947-2272, or visit www.abaretirement.com or write ABA Retirement Funds P.O. Box 5142 • Boston, MA 02206-5142 • abaretirement@us.ing.com. Be sure to read the Prospectus carefully before you invest or send money. 11/2007

Boston Bar Journal

Volume 53, Number 1
January/February 2009

Officers of the Boston Bar Association
President, Kathy B. Weinman
President-Elect, John J. Regan
Vice President, Donald R. Frederico
Treasurer, Lisa C. Goodheart
Secretary, James D. Smeallie

Members of the Council

Lisa M. Cukier
Paul T. Dacier
Anthony M. Doniger
Bruce E. Falby
George P. Field
Laurie Flynn
Lawrence M. Friedman
Elizabeth Shea Fries
Randy M. Gioia
Damon P. Hart
Christine Hughes
Julia Huston
Kimberly Y. Jones
Wayne M. Kennard
Grace H. Lee
James D. Masterman
Wm. Shaw McDermott
Edward Notis-McConarty
Maureen A. O'Rourke
Laura S. Peabody
Mala M. Rafik
Rebecca B. Ransom
Douglas B. Rosner
Charles E. Walker, Jr.
Mark J. Warner

Past Presidents

Anthony M. Doniger
Edward J. Barshak
Joseph W. Bartlett
John G. Brooks
R.J. Cinquegrana
John J. Curtin, Jr.
Gene D. Dahmen
Anthony M. Doniger
John P. Driscoll, Jr.
Thomas E. Dwyer, Jr.
Hugh R. Jones, Jr.
Michael B. Keating
Joseph L. Kociubes
Renée M. Landers
Edward P. Leibensperger
William F. Looney, Jr.
Joan A. Lukey
Hon. James P. Lynch, Jr.
Hon. Sandra L. Lynch
James J. Marcellino
Hon. Margaret H. Marshall
Edward I. Masterman
John A. Perkins
Rudolph F. Pierce
Joel M. Reck
Richard W. Renehan
Lauren Stiller Rikleen
Mary K. Ryan
Richard A. Soden
Raymond H. Young

Boston Bar Journal
Bonnie Sashin, Editor
Aaron J. K. Ostrow, Associate Editor
Catherine F. Meeks, Layout and Cover Design

The *Boston Bar Journal* is published five times a year by the Boston Bar Association at 16 Beacon Street, Boston, Massachusetts 02108. Tel. (617) 742-0615. Articles from the members of the Boston Bar Association are encouraged. Mail all correspondence to the *Boston Bar Journal*, 16 Beacon Street, Boston, MA 02108. Visit the Boston Bar Association at www.bostonbar.org. Articles appearing in the *Boston Bar Journal* represent the views of their authors and do not necessarily carry the endorsement of the Association.

©2009 Boston Bar Association.
All rights reserved.

Advertising inquiries:
Call (617) 742-0615.

Board of Editors
Matthew C. Baltay
Manisha H. Bhatt
Madeleine Blake
Lisa S. Burton
Michael A. Collora
Hon. Judith Fabricant
Donald R. Frederico (Chair)
Hon. Mark V. Green
Joseph Halpern
Martin R. Healy
J. Allen Holland
Kimberly Y. Jones
Elizabeth Eunjoo Kim
Andrea Studley Knowles
Paul G. Lannon, Jr.
Hon. Peter M. Lauriat
Michael K. Loucks
John Loughnane
Martha Ann Mazzone
David A. McKay
Mark F. Murphy
Timothy M. Murphy
Regina S. Rockefeller
Hon. Janet L. Sanders
Kathleen Burdette Shields
Vivian Tseng
Damian W. Wilmot
Hon. Gabrielle R. Wolohojian

Boston Bar ASSOCIATION

Contents

President's Page 2

BBJ Editorial Policy 3

Departments

Opening Statement 4
Web 2.0 and the Lost Generation
By Donald R. Frederico

First Principles 5
Web 2.0: What's Evidence Between "Friends"?
By Seth P. Berman, Lam D. Nguyen and Julie S. Chrzan

New Discoveries 8
The New E-Discovery Frontier — Seeking Facts in the Web 2.0 World (and Other Miscellany)
By Martha A. Mazzone

Heads Up 12
Massachusetts Adopts Comprehensive Information Security Regulations
By Peter M. Lefkowitz

Practice Tips 14
Law Firm Added You as a Friend
By Stephen G. Charkoudian and Kenda J. Stewart

Heads Up 16
What Happens When the College Rumor Mill Goes Online?
By Dana L. Fleming and Joseph M. Herlihy

Vantage Point 18
The Future of Online Networking
By Robert J. Ambrogi

By Kathy B. Weinman

"Send Lawyers, ~~Guns~~, And Money"*



When the bank foreclosed on their building, the Vietnamese-American tenants were fully paid up on their rent. During the foreclosure, however, conditions at their residence had deteriorated; the building had developed extensive leaks and the heating system had broken down. The tenants — including the elderly and disabled — nevertheless persevered. When the bank sought to evict them, they called Greater Boston Legal Services for help. A staff attorney, Zoe Cronin, led their successful defense. After exploring all avenues of redress, Cronin negotiated an agreement with the bank entitling the tenants to a one-year lease at reduced rent, an option to purchase the building, and compensation exceeding $40,000 for the conditions they had endured.

These tenants were fortunate. They had a lawyer. In normal times, legal services programs in Massachusetts turn away over one-half of qualified callers in need of help as a result of inadequate resources.

But these are not normal times. Funding for legal aid in the Commonwealth of Massachusetts is in crisis. In recent years, revenue generated by attorneys' Interest on Lawyers' Trust Accounts ("IOLTA") has comprised over one-half of the financial support for legal services in the state. Established by the Supreme Judicial Court in the late 1980's, the IOLTA program requires lawyers holding clients' funds for a short time or in nominal amounts to deposit them in special interest-bearing accounts. Most of the interest earned on those accounts is distributed to legal aid programs that serve the poor and the elderly throughout the Commonwealth. As a result of the dramatic drop in interest rates and the decline in the number of real estate and other transactions, revenue generated by IOLTA for legal aid is projected to plunge by 54% this fiscal year alone.

The drop in IOLTA revenue has already translated into an unprecedented decline in the availability of legal services. The Massachusetts Legal Assistance Corporation ("MLAC"), the largest funding source for civil legal aid in the Commonwealth, was forced to slash its general support grants to legal services by nearly 40%, from $22 million last fiscal year to $13.5 million this year. MLAC drained its reserves of its last $3.5 million to do so, leaving no cushion for next year. Greater Boston Legal Services has already cut its budget by 13.5%, Neighborhood Legal Services by 29%, and Western Massachusetts Legal Services by 27%. It is estimated that 20,000 fewer people in desperate need will be served as a result.

These cuts come at a time when the need for legal aid has never been greater. People are struggling to survive and put food on their tables and shelter over their families' heads. At moments like these, the requests for legal assistance in areas such as unemployment benefits, evictions, bankruptcy and even domestic violence multiply. Neighborhood Legal Services, which serves the poor and the elderly in Essex County, has experienced a 30% jump in calls in recent months. There are too many in need and too few resources to help.

What can — what should — we as lawyers do?

- Write to the governor, your state legislators and legislative leaders to urge them to preserve state funding of $11 million for civil legal services for both the current fiscal year and fiscal year 2010. While maintaining funding at the current level will not bridge the gap caused by the loss of IOLTA revenue, at least it will not exacerbate what are already tragic consequences for the neediest residents of our state. Sample letters can be found on website of the Equal Justice Coalition at www.equaljusticecoalition.org.

- Donate to legal aid programs in your community and encourage your law firm or organization to maintain or increase its contributions to legal aid programs. In fiscal year 2008 alone, law firm and individual donations to MLAC-funded programs totaled $4.1 million. A list of these programs may be found on MLAC's website at www.mlac.org.

- Represent low-income individuals on a pro bono basis. In a recent communication, the Volunteer Lawyers Project of the Boston Bar Association notified pro bono leaders at various Boston law firms that "[o]ver the next few months, we … will be coming to you with more requests for assistance and new projects to address the need," particularly in areas such as "housing, including foreclosures, evictions due to foreclosures, evictions and housing conditions cases; bankruptcy, both chapter 7 and 13; unemployment compensation appeals; and domestic matters, including domestic violence." Say yes when you get the call, but also seek out opportunities to help. The BBA works with organizations such as the Volunteer Lawyers Project to identify volunteer opportunities and train attorneys to handle the work. Check out their websites at www.bostonbar.org/ps and www.vlpnet.org.

We must try to make a difference. In the words of Warren Zevon's song, "The s–t has hit the fan."

**Send Lawyers, Guns, and Money* is the name of a song written by Warren Zevon (© 1978 Zevon Music/BMI)

Board of Editors


Donald R. Frederico (Chair)
Greenberg Traurig


Matthew C. Baltay
Foley Hoag


Manisha H. Bhatt
Greater Boston Legal Services


Madeleine Blake
Greenberg Traurig


Lisa S. Burton
WilmerHale


Michael A. Collora
Dwyer & Collora


Hon. Judith Fabricant
Massachusetts Superior Court


Hon. Mark V. Green
Massachusetts Appeals Court


Joseph Halpern
Blue Cross and Blue Shield of MA


Martin R. Healy
Goodwin Procter

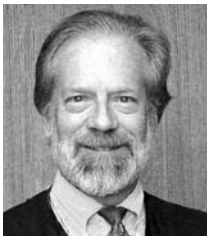

J. Allen Holland
Lynch Brewer Hoffman & Fink


Kimberly Y. Jones


Elizabeth Eunjoo Kim,
McDermott Will & Emery


Andrea Studley Knowles
Sugarman, Rogers, Barshak & Cohen


Paul G. Lannon, Jr.
Holland & Knight


Hon. Peter M. Lauriat
Massachusetts Superior Court


Michael K. Loucks
U.S. Attorney's Office


John Loughnane
Eckert Seamans


Martha Ann Mazzone
Fidelity Investments FMR Corp


David A. McKay
Ropes & Gray


Mark F. Murphy
Wulsin Murphy


Timothy M. Murphy
Bromberg & Sunstein


Regina S. Rockefeller
Nixon Peabody


Hon. Janet L. Sanders
Massachusetts Superior Court


Kathleen Burdette Shields
Choate Hall & Stewart


Vivian Tseng
Welch's


Damian W. Wilmot
Goodwin Procter


Hon. Gabrielle R. Wolohojian
Massachusetts Appeals Court

Statement of Editorial Policy

The *Boston Bar Journal* is the premier publication of the Boston Bar Association. We present timely information, analysis, and opinions to more than 10,000 lawyers in nearly every practice area. Our authors are attorneys, judges, and others interested in the development of the law. Our articles are practical. Our publication is a must-read for lawyers who value being well informed on important matters of legal interest. The *Boston Bar Journal* is governed by a volunteer Board of Editors dedicated to publishing outstanding articles that reflect their authors' independent thought, and not necessarily the views of the Board or the Boston Bar Association.

N.B. Judges serving on the Board of Editors of the *Boston Bar Journal* do not participate in discussions about or otherwise contribute to articles regarding impending or pending cases.

By Donald R. Frederico

Web 2.0 and the Lost Generation



Donald R. Frederico is a Shareholder of Greenberg Traurig, and Co-Chair of the firm's National Class Actions Practice Group. Don chairs the Board of Editors of the *Boston Bar Journal*, and serves as the BBA's Vice President.

Like every senior at the College of Wooster (yes, it's in Ohio and pronounced like "Worcester"), I spent the better part of a year immersed in an intensive research and writing program known as "Independent Study." My major was English, and for a topic I chose to study the influence of the First World War on the writings of three American authors: Ernest Hemingway, F. Scott Fitzgerald and John Dos Passos. I called the project "World War I and the Lost Generation."

Now, more than 30 years later, I find myself on the outer boundaries of a different lost generation, the generation of lawyers who are lost when it comes to new technology. Because Americans my age bring up the rear of the baby boom parade that is swiftly (maybe not so swiftly in this economic climate) marching towards retirement, we are sufficiently adept at technology to master those innovations to which we've had time to adjust, but a little slow to adapt to new ones, and even slower, perhaps, to figure out how they might be useful to our practices. Until recently, we would have thought that Facebook was something you could buy at Borders, that LinkedIn was about golf, and that Web 2.0 was the sequel to the first Spider-Man movie. And just when we think we've got all of that figured out, along comes Twitter to confuse us again.

Yet, to quote Fitzgerald, "we beat on, boats against the current," and discover beneath the surface a vibrant, quickly evolving ecosystem whose inhabitants are tagging each other in photographs and writing on each other's walls. I know this because for several months I have been a virtual card-carrying member of Facebook and LinkedIn, and have friends (even one of my children) in those online worlds. I log on to Facebook at least daily now to read status updates, watch my groups grow, and count the fans of the Boston Bar Association. Sure, as a recovering English major, I cringe that "friend" is now a verb. And once I have performed these limited tasks, I often feel the way I imagine Dustin Hoffman's and Katherine Ross's characters were feeling in the final scene of "The Graduate," wondering "why did I want to be here?" and "now what am I supposed to do?" I'd still rather play Scrabble in three dimensions.

This issue of the *Boston Bar Journal* elevates these mysteries to a higher plane. In a break from convention, we decided to create a thematic issue, focused on how social networking is transforming, and will transform, legal practice. The opportunities that arise from, and hazards created by, engagement in these new forms of human interaction exceed our ability to describe them in this space. Nevertheless, whether you are an experienced or a new member of the bar, a judge, or a law firm marketing or recruiting professional, we hope that you will find here information that will help you navigate this brave new world of social interaction and enrich your professional life. ■

By Seth P. Berman, Lam D. Nguyen & Julie S. Chrzan

Web 2.0: What's Evidence Between "Friends"?



Seth P. Berman serves as Managing Director and Deputy General Counsel of Stroz Friedberg's Boston office.



Lam D. Nguyen is the Director of Stroz Friedberg's Digital Forensics lab in Boston.



Julie S. Chrzan is a Vice President in the Boston office of Stroz Friedberg.

If you are over thirty, you may well have never visited Facebook, MySpace, or Bebo, and the idea of "Twittering," or posting mundane aspects of your life in short and incessant online posts may seem odd, but such social networking sites attract millions of users. They are no longer the sole domain of technologically savvy teenagers. Such Web 2.0 applications host and post untold amounts of personal and professional information about their users, and often serve as the primary means of recorded communication amongst their users. While Web 2.0 pioneers see a fun way to connect to their peers, lawyers are increasingly finding a rich new source of potentially discoverable information. In short, where people go, litigation must follow.

What is Web 2.0?

So what exactly is "Web 2.0"? It may sound like a new version of the World Wide Web, but it doesn't actually refer to any specific new technology. In fact, Web 2.0 doesn't focus on the technology at all, but rather the participatory nature of how a website's content is created and delivered. Web 2.0 applications offer a framework in which its users interact with and even create content themselves, rapidly sharing the information across users and encouraging other users to respond in kind.

This open and dynamic exchange of information radically reduces the level of centralized control that a website owner has over the user experience. It is this very concept that has garnered millions of users rushing to these websites every day. The easiest way to understand this is by contrast to Web 1.0 content. Web 1.0 content is produced, edited, and maintained by the website creator. Thus, Yahoo.com, for example, creates or provides the content available on its web pages. Though Yahoo users had the ability to navigate through that content, they generally lacked the ability to alter it. Web 1.0 is interactive much in the way a television is interactive – the user can change channels, finding content that he or she likes, but the user can not do much to change, comment on, or affect the content he or she finds there.

Web 2.0 applications are designed to give far greater editorial control to users. A simple example of Web 2.0 is a web-based "wiki," the most famous of which is Wikipedia. In wikis, the content is created by users and is dynamic – users are empowered to undo and redo each other's work. Thus, unlike traditional encyclopedias, whose contents are created by a team of experts, Wikipedia entries can be created or modified by any user. Accordingly, if you look up "Boston" in an encyclopedia, you will learn what facts a team of experts thinks is important about the City of Boston. If you look up "Boston" in Wikipedia, you would learn of what an unknown number of individuals – probably many of whom live in or have some interest in Boston – think is relevant and interesting about the city. One significant advantage of the Wikipedia model is that far more data can be compiled through a loose collaboration than could ever be done by a centralized process. Thus, there is a Wikipedia entry for the Boston Bar Association, providing details of the organization, its history and mission, and even a photograph of the historical building it occupies.

Another way in which individuals utilize the interactive nature of Web 2.0 applications is by blogging and commenting on blogs. A surprising number of people publish blogs on every conceivable topic, often revealing quite intimate details of their lives, thoughts, or actions. Though blogs are often written under pseudonyms, some bloggers are quite open about who they are. The distinction could prove important in litigation if the writer's identity is relevant to the issues being litigated. The same analysis applies to people who routinely comment on blogs or in response to articles, even if they themselves do not have a blog.

Perhaps the most talked about Web 2.0 applications are the social networking sites alluded to earlier. Users of Facebook, MySpace and other such sites post comments, pictures, and details about their interests and activities. The contents of these posts can then be shared with "friends," a term that refers to other users who are allowed to access a user's page. Some Facebook users have tens of thousands of

such "friends." Additionally, it is possible to track the "friends" of your "friends," thereby indirectly linking hundreds of thousands of individuals through small degrees of separation. Oftentimes, users are able to see some of the data on pages of the friends' friends, meaning that information on such social networking sites, though at first appearing closed to all but permitted users, often becomes quite widely available. As the user base of these sites has expanded, the sites are no longer limited to talk of college life and twenty-something parties. There is an ever growing array of networking sites that target professionals, such as LinkedIn and Plaxo. All of these sites can have interesting, relevant, embarrassing or just plain titillating information about millions of people, much of which might well be relevant to ongoing litigation.

Another aspect that Web 2.0 sites tend to have in common is that they promote very informal means of communication. As was true for the early days of email (and to a large extent is still true even for emails), electronic communication has a spontaneity that makes it seem impermanent. Thus, people write things in electronic communication that tend to mimic casual spoken conversation rather than formal, written communication. It is for this reason that discovery often unveils truly damning email communications, introduced with statements like "Don't tell anyone about this, but…." This informality is even truer of Web 2.0 applications. Blogs and journal entries on social networking sites are often stream-of-consciousness statements. The perceived anonymity frequently produces much harsher condemnation in response to blogs and articles than is typically acceptable in face-to-face communication. In short, Web 2.0 applications may record people's thought processes and impressions in unguarded moments, exactly the sort of evidence that can be invaluable during litigation.

Potential Value of Web 2.0 Content for Lawyers

The vast amount of user-created content of Web 2.0 applications is a growing resource for lawyers. Many employers routinely conduct web searches on their potential employees as part of background checks. This often turns up the sort of information that more formal background checks would likely miss. For example, an employer might find that an applicant whose criminal record checks and credit history are pristine, may nevertheless be hiding something important in his or her background – such as membership in a neo-Nazi organization. Similarly, in a recent criminal case, pictures on MySpace were credited with being a deciding factor in the sentencing of a then 22-year-old student who received five years and four months in prison after she drove under the influence of alcohol and got into an accident that killed her passenger. Despite a recommendation for probation, the judge decided in favor of a prison sentence after reviewing pictures from the defendant's MySpace page that showed her drinking with friends in the months following the car crash.[1]

These kinds of embarrassing revelations are not limited to people in their twenties. Though it ultimately led to nothing more than a few months of bad publicity, one Web 2.0 application led to an SEC investigation of a prominent CEO. In 2007, the CEO of a popular grocery chain was investigated by the SEC when it became known that he had posted thousands of messages on Yahoo Finance Board promoting himself and his organization (and denigrating competitors and their CEOs) using a pseudonym.

Limiting Discovery of Web 2.0 Information?

Electronically Stored Information ("ESI") decisions in other contexts have established that courts will not hesitate to sanction litigants who fail to turn over ESI because it has been accidentally destroyed or otherwise overlooked.[2] On the other hand, courts want to tamp down on unrestricted "fishing expeditions" amongst the vast expanses of electronically stored information. For example, the defendant in a recent sexual harassment suit sought to compel production of emails from two MySpace accounts, alleging that messages from those accounts might contain evidence that the plaintiff engaged in consensual sexually-related email communications with other persons, of the same type she characterized as sexual harassment in her complaint. In rejecting this argument, the court stated that although the evidence did establish that the two MySpace accounts were indeed the plaintiff's accounts, the defendant had no information concerning the identities of the persons with whom the plaintiff was supposedly exchanging email messages, or the subject matter or content of those messages.[3] However, those seeking to limit discovery of social networking site information shouldn't be overly heartened by this decision, the strong implication of which is that if the defendant had had more evidence that the contents of the websites might have been relevant to the issues, the court likely would have enforced the subpoena.

Collecting and Introducing Web 2.0 Content in Evidence

Once issues such as ownership and scope of the data have been sorted out, attorneys must determine how to introduce evidence derived from Web 2.0 content in court. Although the end result will be different, the steps to be followed for introducing electronic evidence are no different from those for dealing with paper. The correct source of the data must be determined, then the data must be preserved in a defensible manner, authenticated, and deemed relevant to the particular case at bar.

Web 2.0 data, like all data on the World Wide Web, typically can be found in two places. The first is on the server of the website where the data was posted. Thus, one place to obtain data posted on Facebook would be from Facebook itself. Another often overlooked source may be the computer of the user who accessed the website. Indeed, these two sources can work together, with one source augmenting or authenticating the information obtained from the other.

Because the web is dynamic, a website's data cannot be

relied upon for its longevity. Data from websites routinely are altered or deleted altogether. In order properly to preserve a webpage, it must be captured at the exact moment in time in which the preservation is desired. It may also require multiple captures to produce a series of "snapshots," showing how a site changed over time. This can be especially useful in instances where the very fact of habitually updating a website, or the dates and times of the updates, are of evidentiary significance. Once content on a social networking site, blog or wiki has been identified as relevant, it must be preserved in such a way that it can later be authenticated for use as evidence in litigation, as well as to show that a complete preservation was performed. Preservation must be done completely to ensure that all website information – including that which might be contradictory to the stance of a party – is captured.

Web-based evidence can be collected in a variety of ways. With text-based web pages, this can be as easy as pressing the print button and producing the printed pages as "best evidence." For the most part, a fact witness can authenticate the evidence by explaining that she went to the Internet, found the website, and printed what she found. The printed pages can then be entered in evidence without requiring technical expert testimony to introduce complex web concepts.

Of course, websites are rarely restricted to simple text-based pages. Web 2.0 sites rely on rich multimedia content comprised of pictures, video and even sound. This data, especially when user-created, can be a treasure trove of evidence. The preservation of this data, however, is far from simple. It often requires significant technical expertise to faithfully reproduce the information as it would have appeared on the World Wide Web. Will it be sufficient to print stills from a video, or will it be necessary to show the video in its entirety? Can you produce snippets of text from a web posting, or is it only pertinent when shown within the context of the entire website? Can a posted audio file be transcribed, or do you need to introduce it as aural content? From opposing counsel to judges and jury, this data will have a wide audience. It will not only need to be preserved in its original form, but also portable enough to survive the discovery process and to ensure that the relevant parties will be able to review the materials deemed significant.

Additionally, website content such as posted images, documents, and other file attachments may also contain metadata that is crucial in an evidentiary capacity. For example, consider a situation in which an image of illegal activity is found on a group of users' MySpace pages. It may be necessary to determine which of the users originally took the photo. Forensic analysis can reveal metadata in a file that may show details such as the make and model of the camera, the date the picture was taken, or other relevant information, provided that this easily lost data is promptly preserved.

Ultimately, the best evidence will be ineffective if a correlation cannot be shown between the website and the investigative target. Consider a case where an individual is disclosing non-public financial data to a public website. How should a lawyer connect these internet postings to a particular individual or company? While the website may keep a record of the screen name used to make the post, screen names rarely reflect anything more than an anonymous designation. A forensic expert may be able to establish the necessary link between an online posting and a real world individual.

To understand this, it is necessary to understand IP (Internet Protocol) addresses. While a thorough discussion of IP addresses is beyond the scope of this article, it is enough to know that every computer connected to the Internet is designated with a unique numeric address. This is very similar to the phone numbering system. An internet service provider must assign an IP address to a computer before it can access the Internet. Computers require an IP address to determine how to route and transmit data across the World Wide Web. The IP address thus becomes a unique identifier that can pierce the seeming anonymity of the Internet. Knowing how to look for this IP address and knowing whom to subpoena for this information is crucial to authenticate data found on the web. Indeed, attorneys should consider having his or her expert assist in drafting the subpoena to the website to ensure that the necessary information is requested, such as the IP address of the individual who posted the information. An analysis of that website's response will determine who the IP address service provider is, and allow the issuance of a subsequent subpoena to determine the specific computer assigned that IP address at the relevant time.

Depending on the factual circumstances of the case, identifying the computer used to conduct the relevant activity may only be the beginning of the investigation. Assuming that one obtains the appropriate legal authority to search the computer, the question then becomes whether it will still have any useful information. The answer is almost always yes. Since a user unwittingly leaves an evidentiary trail on her computer simply by using it, her computer will provide evidence of her web usage. The user's activity log, time-date stamps of relevant documents, and even deleted files may be able to augment or corroborate evidence located on the website server. What can ultimately be found on a computer is wholly dependent on how often the computer was used, what programs were installed, and how the user interacts with the computer. Computer data is volatile; therefore a forensic exam is far more likely to reveal what a user did on his computer yesterday than what was done three months ago.

Web 2.0 technologies provide fertile grounds for learning more about parties, witnesses and others involved in litigation. Lawyers and judges must know how to find, capture, understand, and utilize this rich new source of potentially discoverable data. ■

(Endnotes)

1 www.dailynexus.com; Published February 1, 2007.

2 *See, e.g., Zubulake v. UBS Warburg LLC,* No. 02 Civ. 1243 (SAS), 2004 U.S. Dist. LEXIS 13574 (S.D.N.Y. July 20, 2004); *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC,* 216 F.R.D. 280 (S.D.N.Y. 2003).

3 *Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc.*, 2007 U.S. Dist. LEXIS 2379 (D.Nev. Jan. 9, 2007).

By Martha A. Mazzone

The New E-Discovery Frontier— Seeking Facts in the Web 2.0 World (And Other Miscellany)



Martha A. Mazzone is a vice president and associate general counsel at Fidelity Investments, in the Litigation group.

Just when you've understood preservation and discovery of email evidence, or instant messages, or, even, "structured data" (as in data in databases) — along comes a new challenge in e-discovery. The author refers, of course, to the various interactive document and communication applications, features and websites known collectively as "Web 2.0," such as "social networking sites," "collaboration software and features," "blogs" and "wikis," to name a few. Remember how we shook our heads over the dumb things people say in email? Welcome to the millennium and the really dumb things people say and do on Web 2.0 sites. (Not that people have stopped using email to say dumb things.)

Warning to reader: Much like surfing a social networking site, writing about e-discovery issues in new media can lead to sidebars, tangents, and less than linear thinking. Go with the flow.

The Basics

Know the technology.

The "data map," which classically depicted a PC, a server, and a firewall, is a dated concept. Query how one "maps" data when documentary evidence can be shared and stored on thousands of Web 2.0 sites and applications online? Your client may keep documents on a file share and e-mails in an archive — easy to map, but now you have to ask your client about messages exchanged during an in-house WebEx meeting in which a key document was displayed, or whether there's a MySpace page. Think big, unorganized and unmappable when framing questions. What virtual meeting technologies are used? Does your client blog, and if so, where? Do document management systems such as Documentum have chat and whiteboarding features available, and do people in the company use them? Where is data stored and in what format?

As litigators, we need to know the bad with the good. What if your client in a business dispute is posting defamatory comments about the other business on a well-known blog? It happens often — ask the small business owners you know about Yelp, Craigslist blogs, and other consumer and community chat, and you will see the blood spilled in these venues between business competitors. If you don't explore these sources, there's a chance your opponent will quickly find out something you didn't know.

Tangent: *Biegel v. Norberg*, a California case filed in February 2008 (Superior Court, County of San Francisco, case no. CGC-08-472522), involves a chiropractor who sued a former patient for defamation and false light invasion of privacy based on the patient's critical Yelp postings. Norberg, the former patient, attempted to turn his defense into a freedom of speech *cause célèbre* and even has a website to raise money for legal fees. Massachusetts cases on defamation, copyright infringement, and free speech on Web 2.0 media are available at the outstanding website and database run by the Citizen Media Law Project, www.citimedialaw.org.

Have a technology partner.

Working on e-discovery issues without a technologist is guaranteed to slow you down and likely to cause errors. That's not to say that you need to hire anyone in particular — your client might have an employee who can walk you through the intricacies of collaboration sites or interactive applications, or you may have a technologist in your law firm. But, as with ESI (Electronically Stored Information) in general, having someone on your team who knows his/her way around a motherboard, or Twitter, is one key to success.

Related sidebar: One possible solution to the problem of authenticating material found on Web 2.0 sites: Images of web pages that receive "cryptographic fingerprints" and are linked to the authenticator's unique voice. *See* www.myelectronicevidence.com. Sufficiency of the authentication is untested, but this example illustrates one

FIND US ON

facebook®

www.facebook.com

Search for
the Boston Bar Association

way in which technology partners are working to solve evidentiary problems in litigation.

Prevention — Avoid e-discovery disasters through thoughtful records management and destruction programs.

Start with the premise that, as with e-mail, people do not immediately understand the permanence of their participation in new media. Records retention policies and programs should seek to reduce the risk posed by incautious users, through destruction of content wherever possible, as soon as possible. If the content in these applications or websites does not have to be retained for operational, regulatory, or litigation hold purposes, prompt and regular destruction should be the policy.

If you are seeking discovery, ask what the company's records retention policies and archiving procedures are for Web 2.0 applications and features. Your opponent may inadvertently save more information than it needed to or intended. And if you represent one of those companies, such information may be subject to preservation and discovery obligations just as other business records of the company are. Trying to figure out how to preserve and discover information after the technology has been built and is in use will be difficult.

Best Practices: Yahoo has blogger guidelines for its employees. *See* http://jeremy.zawodny.com/yahoo/yahoo-blog-guidelines.pdf, reminding them that they are legally responsible for their postings ("Outside parties actually *can* pursue legal action against you (not Yahoo!) for postings.").

Finding and retrieving evidence in Web 2.0 applications, sites and features

Courts and opponents are not likely to buy the argument that most electronic data is inaccessible, because, in fact, it's really not true. Excellent search and categorization engines, along with sophisticated fast data storage, have practically eliminated burden arguments based on the difficulty and cost of accessing email and other electronic evidence. (Take heart — you still have cost of review arguments.)

Not so, however, when it comes to Web 2.0. Thus far, although searchability exists as it does for any website or application, the form of Web 2.0 content makes it harder to pinpoint relevant evidence in a massive amount of data. Accessibility, as this term is understood in the electronic discovery Federal Rules, is definitely an issue when it comes to content on Web 2.0 applications and sites.

The counterargument says that Web 2.0 is about who creates the content, not the technology itself. It is true that the basic technology is really no different from Web 1.0. But the twists and turns of figuring out how Web 2.0 content is classified in a way that allows it to be searched — and what can be retrieved from a search — can cause migraines. What is the "communication" in a blog and where does it begin and end? Who is a "custodian" or a sender or recipient in an anonymous blog or a wiki? Think about a corporate collaboration site where documents are edited on the site over a period of weeks. Retaining hundreds of archived web pages is not that difficult, unfortunately, but finding your evidence in the morass using the old paradigm of search terms and custodians just may not work. Still, you are probably going to have to, and want to, look.

In his book, *Everything Is Miscellaneous: The Power of the New Digital Disorder*, author David Weinberger makes the point eloquently: "our homespun ways of maintaining order are going to break — they're already breaking — in the digital world." His book is not about e-discovery *per se*, but its thesis — the digital world classifies information, if at all, in new and different ways — is relevant to the task of finding a needle of evidence in a haystack of data.

Another reason identifying custodians in new media may be difficult is the issue of anonymity. The ability to say what you think anonymously is prized by new media users, but it affects the very notions of fairness in our justice system. The term "discovery" itself bespeaks an expectation of attribution and disclosure. Many, if not most, of our fact-finding endeavors are based on the identification of wrongdoers, witnesses, and owners of information. But take the example of a Web 2.0 defamation lawsuit where the blogger is unknown. Lawsuits

against John Does are nothing new, but the Does' right to anonymity is a hotly defended feature of the Web 2.0 user community.

Boston's own Aerosmith frontman Steven Tyler has filed one such lawsuit, *Steven V. Tallarico, p.k.a. Steven Tyler v. Does 1-20*, in California Superior Court (County of Los Angeles, case no. BC398715), alleging public disclosure of private facts, false light, and misappropriation of likeness by a person or persons who impersonated him online. Google took down the fake Tyler blog from its Blogspot, at Tyler's request, but Tyler went further and asked for the unmasking of and an injunction against future impersonation by the individual Does 1-20, inclusive.

The case also touches on third-party discovery in the Web 2.0 world. Tyler needs Google to reveal the identity of Does 1-20. One fairly recent Massachusetts federal district court case addressed the standard for forcing an internet service provider to reveal the identity of an anonymous poster. In *McMann v. Doe*, 460 F. Supp. 2d 259 (D. Mass. 2006), plaintiff McMann, a Massachusetts real estate developer, alleged that a website posted by an anonymous individual defamed him and invaded his privacy. The plaintiff tried to obtain the identity of the individual. The court disposed of the matter on diversity jurisdiction grounds, because the anonymous defendant's citizenship was not known. But, the court also provided alternate grounds for dismissal, holding the plaintiff to a summary judgment standard of evidence of his claims of harm, in order for the plaintiff to force a third party to disclose the anonymous "speaker's" identity.

If this topic of anonymity interests you, there's plenty more to read. The Web 2.0 community is nothing if not vocal about legal threats to its vision of true free speech online — and naturally, materials are all available online. In addition to the Citizen Media Law Project, you might want to look at the websites of the First Amendment Center in Nashville, Tennessee (at Vanderbilt University), the Electronic Frontier Foundation in Washington, D.C., and the website of our own Northeastern University's just-founded New England First Amendment Center.

Take heart — although new media forms may involve new paradigms, struggling with the search for electronic evidence is hardly new. In fact, you probably already have a good idea about your approach to discovery in new media. But here are a few tips to consider:

- Think about your definition of "communications" in document requests. Boilerplate might not be effective if you need to call out Web 2.0 sites and features specifically.
- Don't give up if you meet with resistance from an opponent — or your own client — when seeking data that is not organized by custodian or that cannot be easily loaded into Concordance. There may yet be no standard efficient way to retrieve content in new media sites, but call in that technology partner and see what you can come up with. Maybe the system logs user identification information. If so, you may be able to trace and identify users by name. (Hint — if your client has a corporate security office, it might be your best technology partner for that task.) Most sites are text-searchable at least.
- Companies have technology disaster recovery plans — maybe they saved PDF'd web pages, or captured blog threads daily in simple, searchable text.
- Some companies capture the navigation data of their website users — using that information, target who looked at what information on a blog, and when.

Think Like A User

Doing any kind of research includes determining which paths to follow and when to stop following them. Discovery on Web 2.0 sites is no different, really. The paths are harder to define, some of them have obstacles we might not have encountered in traditional research, and maybe it's too easy to get re-directed onto another path — but if we embrace the challenge and learn to think the way bloggers and new media moguls think, this discovery labyrinth can be conquered. ■

By Peter M. Lefkowitz



Peter M. Lefkowitz is Vice President and Chief Counsel, Privacy & Security for Oracle Corporation and co-chair of the Boston Bar Association's Privacy Law Committee. Mr. Lefkowitz works in Burlington, Massachusetts.

Massachusetts Adopts Comprehensive Information Security Regulations

As of 2009, all businesses that use or store personal information of Massachusetts residents are required to comply with security regulations published by the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR). *See* 201 C.M.R. 17.00. Titled "Standards for The Protection of Personal Information of Residents of the Commonwealth," the regulations set out the most comprehensive information security requirements by any state to date.

In 2007, Massachusetts joined 38 (since raised to at least 44) other states in enacting data breach notification legislation. Chapter 93H requires entities that "own or license" personal information of Massachusetts residents to publicly report the unauthorized acquisition or use of unencrypted data. As with other laws aimed at identity theft, the statute defines personal information narrowly as an individual's name plus either Social Security, driver's license, state-issued identification card, credit card or financial account number. Though the reporting obligation varies in some respects from other state laws — most notably in its limitation on which details of a breach may be disclosed to consumers — the law is generally consistent with others in terms of when reporting is required, timing of the notice, and exceptions for law enforcement activities.

Where the Massachusetts law differs dramatically is its inclusion of provisions mandating the adoption of detailed information security regulations for both businesses and government. The statute enumerates specific objectives for the regulations:

> ensure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

Thus, the Legislature clarified that, beyond using notifications to shine a light on individual breaches, the intent of the statute is to establish protections that reduce the need for such notifications.

The resulting business regulations impose detailed administrative and technical obligations on any "person" — any individual or entity, whether or not operating in the Commonwealth, that is not an executive, political or other office of Massachusetts government — that "owns, licenses, stores or maintains" personal information of Massachusetts residents. Here alone, the breadth of the regulations is significant: they extend to any individual, for-profit entity or

non-profit entity that holds or processes personal information of a Massachusetts resident.

The regulations' administrative obligations include maintaining and enforcing a detailed information security program and creating policies governing whether and how employees keep, access and transport records; limiting personal information collected in any instance to what is reasonably necessary for the original purpose of collection; and regularly monitoring to ensure that the security program is operating effectively. Persons (as defined) also are required either to identify all records, computers, computer systems, and storage media that may hold personal information or to treat all such records and systems as though they contain personal information. And persons are instructed to pass on all of the administrative requirements, as well as the technical requirements discussed below, to any third-party service providers with access to personal information. More pointedly, the regulations require persons to obtain a written certification of compliance from each service provider.

Separately, the regulations establish technical requirements for any computers, systems and networks involved in maintenance or transmission of personal information. These include use of individual account identifiers to limit access; secure measures for selecting, storing and accessing passwords; and system monitoring to detect unauthorized access to or acquisition of information. As well, all personal information must be encrypted when stored on laptops or other removable devices and in transit across public networks (most transmissions beyond an entity's firewall) or by wireless connection. Notably, the definition of "encryption" has been broadened to permit non-algorithmic means of protecting information, such as anonymization or hashing, so long as those measures provide the same level of protection as encryption.

Apparently conceding to concerns raised in response to an earlier draft, the final regulations attempt to balance compliance with business needs, most visibly in the selective use of a reasonableness standard. For example, persons must use "a *reasonably* secure method of assigning and selecting passwords," conduct "*reasonable* monitoring of systems," and employ "*reasonably* up-to-date firewall protection" and "*reasonably* up-to-date versions of system security agent software." Further, compliance with the regulations' obligations will be judged in light of an entity's size, scope and resources and the amount and type of data at issue.

Though the regulations initially were slated to take effect on January 1, the deadline for compliance recently was extended to May 1; the deadline for encryption of portable devices and for obtaining service provider certifications is now January 1, 2010. OCABR has published a number of documents to assist businesses with their compliance efforts, including frequently asked questions, a compliance checklist, and a guide for small businesses. All are available from the Office's official web site.

Various states have enacted elements of the Massachusetts regulations. Nevada requires encryption of personal information in transit; New York, Michigan, Texas and others have restricted publication and/or use of Social Security Numbers; and Minnesota has enacted security controls for payment card information. But no state has gone as far as Massachusetts in regulating precisely how businesses protect personal information — yet. ■



Mediation/ Arbitration Services by a practicing trial lawyer

Jeffrey S. Stern

Fellow and Member, Board of Directors of the American College of Civil Trial Mediators

- Business
- Employment
- Personal Injury
- Construction
- Insurance
- Product Liability
- Medical Malpractice
- Professional Malpractice
- Partnership Dissolutions
- Intellectual Property

SRBC **SUGARMAN, ROGERS, BARSHAK & COHEN, P.C.**
Attorneys at Law

101 Merrimac Street, Boston MA 02114-4737 • 617-227-3030
617-523-4001 Fax • stern@srbc.com

By Stephen G. Charkoudian and Kenda J. Stewart

Law Firm Added You as a Friend



Stephen G. Charkoudian is a partner and chair of Goodwin Procter's IP Transactions & Strategies Practice and a member of the firm's Technology Companies Group. His practice encompasses a broad range of technology transfer and intellectual property matters.



Kenda J. Stewart is an associate in Goodwin Procter's Business Law Department and a member of the firm's IP Transactions & Strategies Practice.

In a world where whom you know counts almost as much as what you know, social networking sites are changing the dynamics of business relationships. What began as a fad amongst college students and musicians is now burgeoning into multiple online forums where entrepreneurs, executives, and other professionals from around the globe can establish and maintain business relationships. While the traditionally conservative legal profession has been slow to jump on the social networking bandwagon, law firms should note that social networking sites such as Facebook, LinkedIn and Twitter provide low-cost opportunities to grow and stay competitive in both the legal and client marketplaces.

Legal Recruiting

Social networking sites can bolster a firm's legal recruitment efforts by providing a means to distribute information about the firm and the summer clerk program to law students and junior lateral hires that accurately reflects the firm expertise and culture. While it has a decidedly more "grown up" tone than other social networking sites (e.g., MySpace), Facebook's university roots, tools, and demographic profile make it the likeliest candidate for these purposes. Law firms can create a "Facebook Page," on which they can post information and photos, and create invitations to events. Law firms can also create "groups" on Facebook geared towards recruiting (e.g., "Summer Associates 2009"). Information located on a firm's Facebook page or Group page can become key information to law students struggling to differentiate among firms.

LinkedIn can also be an effective recruiting tool because it allows law firms to scope out potential lateral hires at the mid- or senior-level, and to obtain an idea of their connections, current employment status, and areas of expertise.

Cultivating Junior and Mid-Level Associate Connections

Junior and mid-level associates should be encouraged to develop and maintain relationships with contacts they make early in their careers so that, as they become more senior, these relationships become connections with key decision makers. LinkedIn can be a helpful tool in

that effort. Junior and mid-level associates can also utilize LinkedIn to showcase their educational and professional achievements, and build up the firm employee list as one that includes skilled and diverse professionals.

Junior and mid-level associates can also use social networking sites to establish their interests in particular areas. Facebook allows associates to join groups targeted to their areas of interest, post links to articles or blogs discussing their areas of interest, and engage in online discussions with other users about postings on their profiles related to those areas of expertise. Twitter enables users to microblog on a specific industry, which might include a liveblog of a particular conference or just periodic updates on the goings on within particular areas of expertise.

Business Development

At the leadership level, partners can use social networking sites to generate prospective client leads, strengthen existing client relationships, and monitor clients' activities and those of their competitors. For instance, partners can use LinkedIn to create a robust network of their clients' key decision makers. LinkedIn provides credibility by association, where a strong network of industry leaders instills confidence in current and prospective clients. LinkedIn has also become a tool for business introductions. Members can search the site for other members who work for a particular company and can see how they may be connected. With the recently released company profiles feature, users can not only see whether anyone who works for a particular company is in their network, but can also see listings of the individuals at that company who are highlighted because they may be actively in the news, referenced in blogs, participating in industry groups, and/or frequently the result of searches and other activities within the LinkedIn network.

Partners can also use social networking sites to perform diligence on current and prospective clients, by keeping up to date on their activities and monitoring their overall impression in the marketplace. Sites like Facebook, with fan pages and group functionality, can provide information on how users view a company and its competitors. Sites like Twitter can also provide useful information in this regard, especially if it is possible to find a particular Twitter feed that is directly related to a client's industry. Twitter can often provide a good "first reaction" analysis if a client is, for instance, releasing a new product or announcing earnings.

Pitfalls to Avoid

While law firms can use social networking sites in many significant ways, they should take care to avoid the pitfalls associated with the use of such sites. For example:

Personal Networking v. Professional Networking:

Users must take care that their personal social networking site does not reflect poorly on their employer or on their own character.

Maintaining "One Voice": Firms that set up an online presence, either through a social networking site, a firm blog, or a Twitter feed, must take care to project a consistent "voice." A firm's postings should conform in overall style and should not appear disjointed.

Disclosing Information: Firms that make regular postings on a social networking site regarding important transactions in which they have been involved must take care that they do not disclose any potentially sensitive information.

Attorney Client Relationship: On sites like Facebook, which encourage lively interactive discussion, firms must be careful not to engage with other users in a way that may be seen as giving legal advice such that an attorney-client relationship is established.

Conclusion

Social networking sites can provide important tools that law firms can leverage to recruit and cultivate skilled internal teams and to generate business. Participating in social networking sites is a low-cost activity that has the potential to reap real rewards if utilized correctly. That said, while social networking sites can provide the jumping-off points for new relationships, they are by no means short-cuts past the effort and energy that must be put in to developing lasting business relationships. LinkedIn may get you in the door, but it's the person behind the profile that will get you the deal. ■

By Dana L. Fleming and Joseph M. Herlihy

What Happens When the College Rumor Mill Goes Online?

Privacy, Defamation and Online Social Networking Sites



Dana L. Fleming is an associate in the Wage & Hour Litigation Practice Group in Seyfarth Shaw's Boston office.



Joseph M. Herlihy is General Counsel at Boston College and formerly served as co-chair of the BBA College and University Law Section.

While student participation in online social networking communities is prevalent, case law on this subject remains scarce. Nearly five years into the online phenomenon that began with the founding of Facebook in 2004, colleges continue to confront the legal implications of these sites with limited tools or guidance from courts, regulators or lawmakers. The result has been a mix of policy decisions that range from the draconian (*e.g.* university expelled *over*-age graduate student for posting picture on MySpace that showed her at a Halloween party drinking from an opaque cup with a caption that read "Drunken Pirate") to the mundane (*e.g.* colleges use social networking sites to reach out to prospective students and young alumni, often by creating fictional pages for the school mascot).

The two social network giants, MySpace and Facebook, boast more than 100 million users worldwide. Students post and share personal information with "friends," including pictures, personal descriptions, music and video clips, blogs, relationship status updates, sexual orientation, club and sports affiliations, and details about their day-to-day activities, real and imagined. Although the sites offer a range of different privacy settings, it is not uncommon for users to have hundreds or even thousands of "friends," a significant percentage of whom are, according to a recent survey, total strangers. In this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking. When warned that prospective employers might well review Facebook pages, students at one school protested that such use would be an invasion of privacy. Apparently, the employers "did not get the memo."

Prosecutors and judges have used postings to argue for or to impose harsher punishments where the defendant's profile demonstrated a clear lack of remorse. In a fatal drunk driving case in Rhode Island, prosecutors used pictures of the driver at (another!) Halloween party dressed in an

orange jumpsuit labeled "Jail Bird" to argue successfully for a longer sentence. This trend has been paralleled in student disciplinary hearings where the traditional display of contrition is now frequently countered with Facebook screenshots. Colleges have also started to use personal websites as the basis for student disciplinary charges. In October 2005, a student at Boston's Fisher College was reportedly expelled for defaming a college police officer on Facebook. In March 2008, a freshman at Ryerson University was expelled after the school learned he was hosting a "Facebook study group" that solicited homework answers online.

Many student life administrators have asked their counsel if they should monitor students' "virtual lives," assuming, perhaps naively, that they can accurately identify the source of offending content or rely on posted information. Like any medium in the digital era, postings and photographs from social networking sites can be distorted. Moreover, new campus chat sites, like Juicy Campus, "guarantee" anonymity, making it difficult for schools to identify students who are posting inappropriate material, short of undertaking a review of students' computer logs, a measure restricted under most university IT policies to investigations of serious improprieties.

As any Psych 101 student would predict, an increased sense of online anonymity breeds outrageous and defamatory posts. The few Juicy Campus discussion threads that can be printed in this journal invite nominations for such categories as "dumbest Duke student," "guys with STDs," and "cutest non-slutty sorority girl." The rest are disturbing enough to have spurred a backlash among the normally jaded campus population. A few factors have combined to create this perfect devil's playground. Section 230 of the Communications Decency Act of 1996 shields the site operators from defamation claims by precluding them from being treated as "publishers." The gossip entrepreneurs encourage defamatory postings with promises of anonymity. "C'mon. Give us the Juice! Posts are totally, 100% Anonymous," barks the Juicy Campus website; but when invited to speak at Georgetown, its founder Matt Ivester piously described his site as a censorship-free vehicle for "letting students talk about the things that interest them most."

Despite many requests from students and parents, and precedent establishing that a campus network is not a public forum under First Amendment analysis, no college or university attempted to block access to Juicy Campus until Tennessee State University did so this November. The core value of academic freedom is reason to hesitate, and IT administrators will admit that such attempts are largely ineffective. For now, educating students about the consequences of on-line behavior is perhaps the only tool our college and university clients have to help their campuses navigate the online rumor mill. ■

SRBG
ATTORNEYS AT LAW

Litigation Associate

Prominent regional law firm seeks associate with one to three years experience for immediate position in our busy litigation department in our Manchester, NH office. Qualified candidates must have demonstrated excellence at both the undergraduate and law school levels, exhibit exceptional writing and communication skills, and possess the initiative and motivation to succeed in our fast-paced professional environment. Our associates enjoy top-of-market salaries, generous benefits, work-life balance, and a partner track of seven years.

To be considered, submit resume, writing sample, and undergraduate and law school transcripts in confidence to Robert H. Miller, Hiring Partner, 1000 Elm Street, Manchester NH 03105-3701 or electronically to rmiller@sheehan.com. Admission to the New Hampshire Bar will be required but is not a prerequisite to hiring.

By Robert J. Ambrogi

The Future of Online Networking



Robert J. Ambrogi is a lawyer and consultant in Rockport, Mass., concentrating in media, technology and dispute resolution.

Over the past several years, many lawyers have used so-called "social networking" sites to connect with colleagues and clients. Sites such as Facebook, Twitter and LinkedIn have allowed attorneys (and others) to build a community of connections. Indeed, social networking sites have supplemented and, for some lawyers, supplanted traditional network building activities

No crystal ball is needed, however, to see that the future of these sites, at least within the legal profession, promises more than mere connections. Networking will remain a key part of the picture, but as more sites compete to serve the legal profession, they will offer more diverse and practical suites of tools.

Networking sites will morph into broader, online communities for legal professionals. Along with connections, they will offer community, content and collaboration. They will be places where lawyers will not simply network with each other, but also work with each other and share resources with each other in more substantive ways.

The reason no crystal ball is needed is that this future is already visible. Two projects now underway, Legal OnRamp and Martindale Hubbell Connected, reveal a new breed of site, where networking is only part of the equation. These multilayered sites aim to become powerful resources for lawyers to use in building and managing their practices.

It was this very desire to meld networking, content and collaboration that gave birth to Legal OnRamp, www.legalonramp.com, a site open only to members of the legal profession. The general counsel of nine blue chip companies sought to create a network to automate collaboration and content-sharing among in-house and outside counsel. They wanted a site open to a broad cross-section of lawyers but also with secure areas for private interactions.

Legal OnRamp cherry-picked the best features from multiple platforms: extranets, Facebook, news aggregators, research libraries, document-management systems and even the proverbial water cooler. It is free to join, but private-firm lawyers are asked up front to contribute a substantive legal article or FAQ to be shared with other members.

Legal OnRamp resembles networking sites such as LinkedIn in that it centers on members' profiles and connections. Unlike other sites, however, Legal OnRamp emphasizes content as strongly as connections. Its offerings range

from various news and blog feeds to more substantive libraries of research materials and legal forms.

Within this superstructure, members can create private areas, called "ramps," with their own networking components, libraries and collaboration tools. Cisco's legal department has one, for example, used by its in-house and outside lawyers. It includes a database of its contracts and another of its patents, among other items.

Another site where the future can be seen today is Martindale Hubbell Connected, www.martindale.com/connected, now operating in a limited, beta version. The final version, due in early 2009, promises a range of features designed to keep professionals engaged and enhance their productivity.

As with Legal OnRamp, networking will remain a key component. In fact, by tapping into the full Martindale-Hubbell database of more than one million lawyers worldwide as well as the research database of its parent company, LexisNexis, the site promises to offer networking options unmatched by other sites.

Members will see their professional networks paired with the full Martindale directory. Thus, if a member searches Martindale for a litigation attorney in Boston, the results screen will display a "My Network" tab showing lawyers who both match the search and are within the member's first- and second-degree network. By tapping into case reports in LexisNexis, it will also show whether you ever litigated with or against the lawyer.

Like Legal OnRamp, Martindale Hubbell Connected will allow members to create controlled-access "communities." Communities can be customized to feature content from a variety of sources as well as discussion groups, forums, blogs and webinars. The site will also feature a Wikipedia-like legal reference, written and edited by members, but "pre-seeded" with articles from the Martindale-Hubbell Law Digest.

In December, the American Bar Association launched a networking site of its own in beta, Legally Minded, www.legallyminded.com. . Like these other sites, its goal is to combine networking with a broad range of practical tools and resources – many drawn from within the ABA.

Even without a crystal ball, these sites reveal a future in which on-line professional networking will offer lawyers opportunities to both give and receive, to share their own knowledge and expertise in return for opportunities to tap into the knowledge and expertise of colleagues throughout the world. As these sites show, that future is already here. ■

Save These Dates!

13th Annual Superior Court Bench Meets Bar Conference
Thursday, February 26, 2009

19th Annual Bankruptcy Bench Meets Bar Conference
Thursday, May 14, 2009

Justice is Sweet
Thursday, June 25, 2009



The BBA is here to help.

Boston Bar Association membership has always been a great value. If your professional situation has recently changed, or if you're facing or contemplating a transition, your BBA membership is more important to you now than it's ever been — as a tool to help you keep abreast of developments in practice and the law, and as a way to stay in touch with colleagues and friends.

If membership dues pose a barrier to your continued participation in the BBA, call us today at (617) 778-2040 x3 or email us at membership@bostonbar.org. We'll waive your membership dues and renew your membership.

You've supported us when we needed it.

Now, it's our turn.

Boston Bar
ASSOCIATION



EXPERIENCE THE RIGHT PARTNERSHIP™

ACCESS. EXPERTISE. SERVICE. Together, these powerful advantages form the cornerstone of the Northern Trust experience.

When you work with Northern Trust, you and your clients have access to a community of knowledge, innovation and fresh perspectives, delivered with the personal attention of our tenured professionals.

Built from a fiduciary heritage of putting our clients' best interests first, we complement your expertise with a complete array of banking, investment management and trust and estate services – as well as specialized solutions in areas such as philanthropy, family business and real estate – so you can address virtually any complex issue faced by your clients.

To learn more about how we can work together to help your clients achieve their financial goals, contact Lee Woolley at 617-235-1822 or ljw2@ntrs.com. You may also visit our dedicated website for professional advisors at northerntrust.com/wealthadvisor.

WILL & TRUST FORMS — A VALUABLE RESOURCE

Northern Trust's *Will & Trust Forms* addresses a wide variety of situations facing today's legal professionals, helping you serve your clients more efficiently. Available in hard copy or Web-based format, this valuable resource provides everything you need to personalize documents quickly and easily. Simply contact us via email at will&trustforms@ntrs.com.

Northern Trust

One International Place, Suite 1600 • Boston, MA

Private Banking | Asset Management | Financial Planning
Trust & Estate Services | Family Office Services | Business Banking

Boston Bar
ASSOCIATION

16 Beacon Street
Boston, MA 02108

Prsrt Std
U.S. Postage
PAID
Boston, MA
Permit No. 57557

THE BOSTON BAR ASSOCIATION SALUTES ITS SPONSORS HELPING US ADVANCE OUR MISSION

Anderson & Kreiger LLP
Bingham McCutchen LLP
Blue Cross & Blue Shield of Massachusetts, Inc.
Boston Medical Center
Boston Redevelopment Authority
Bromberg & Sunstein LLP
Brown Rudnick LLP
Burns & Levinson LLP
Choate, Hall & Stewart LLP
Committee for Public Counsel Services
Conn Kavanaugh Rosenthal Peisch & Ford, LLP
Davis, Malm & D'Agostine, P.C.
Day Pitney LLP
Dechert LLP
DLA Piper US LLP
Donnelly, Conroy & Gelhaar, LLP
Duane Morris LLP
Dwyer & Collora, LLP
Edwards Angell Palmer & Dodge LLP
Foley Hoag LLP
Foley & Lardner LLP
Gesmer Updegrove LLP
Goodwin Procter LLP
Goulston & Storrs, A Professional Corporation
Greater Boston Legal Services
Greenberg Traurig LLP
Hanify & King, P.C.
Hemenway & Barnes
Hinckley, Allen & Snyder LLP
Hirsch Roberts Weinstein LLP
Holland & Knight LLP
Lawyers' Committee for Civil Rights
Legal Advocacy and Resource Center
Looney & Grossman, LLP
McDermott Will & Emery LLP
Michaels, Ward & Rabinovitz, LLP
Mintz Levin Cohn Ferris Glovsky & Popeo P.C.
Nixon Peabody LLP
Nutter McClennen & Fish, LLP
Office of the Attorney General
Office of the Corporation Counsel, City of Boston
Law Department
Partners HealthCare
Peabody & Arnold LLP
Pepe & Hazard LLP
Rackemann, Sawyer & Brewster,
Counsellors at Law
Robins, Kaplan, Miller, & Ciresi L.L.P.
Robinson & Cole LLP
Ropes & Gray LLP
Sherin and Lodgen LLP
Shilepsky O'Connell Hartley LLP
Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates
Sugarman, Rogers, Barshak & Cohen, P.C.
Sullivan & Worcester LLP
Todd & Weld LLP
Verrill Dana LLP
Weil, Gotshal & Manges LLP
Wilmer Cutler Pickering Hale and Dorr LLP
Yurko, Salvesen & Remz, P.C.

Professional Excellence **Facilitating Access to Justice** **Serving Our Community**