THE BOTTOM LINE
www.calbar.ca.gov/lpmt
OFFICIAL PUBLICATION OF THE STATE BAR OF CALIFORNIA LAW PRACTICE MANAGEMENT AND TECHNOLOGY SECTION

LOSING THE EXPECTATION OF PRIVACY BIT BY BIT, BYTE BY BYTE

By Mark S. Adams

Mark S. Adams

MCLE CREDIT

After reading this article, you can earn MCLE credit by completing the test online

For a generation that has become exceedingly facile with electronic gadgetry and desensitized to the massive amounts of data this gadgetry produces, it perhaps comes as no surprise that video surveillance and on-line monitoring by employers of present and potential employees' electronic profiles and fingerprints have become the norm.

Billions of emails are sent and received every day. Facebook has over 750 million active users, Twitter more than 75 million users, and YouTube boasts more than 24 hours of uploads every minute, every day, with over 2 billion viewers daily. Closed circuit digital video cameras are commonplace, from office security cameras to ATMs. All of this data can be available for review and analysis by friend or foe, including current and potential employers.

Social Media

Law firms now routinely vet their recruits through the Internet—not just before a formal offer is given, but before even taking an interview. Social media sites provide firms with the kind of information about candidates that was simply unavailable from any source just a few years ago. A firm can now easily get a glimpse of a candidate's off-duty persona to help determine if there will be a good fit. For example, an Internet-chatty candidate may say some nasty things about his or her former firm that would never appear on a resume; perhaps express an ambivalence about the field of law; show an

continued on page 2

Our Mission: To Improve the Quality of Law Practice Through Effective Management and Technology

Our website can be found at www.calbar.ca.gov/lpmt — to register for MEMBERS ONLY section see page 16.

MCLE CREDIT

After reading this article, you can earn MCLE credit by completing the test online

unhealthy appetite for engaging in high risk, dangerous activities; or flaunt an illicit, drug-friendly lifestyle. In short, the Internet may reveal a person who is far different than the well-dressed, firm-handshaking, smiling face that's sitting in the lobby waiting for his or her interview. Absent the use of this Internet vetting process for the purpose of unlawful discrimination, at present, law firms are free to make such Internet investigations without any legal repercussions.

Unlike potential employers, current employers have always kept an eye on their employees, and rightly so, because employers suffer the cost of such behaviors as employee theft and various kinds of employee mishaps and indiscretions. Although social media provides current employers with that same window into their employees' lives—a window voluntarily opened by employees when they post things on a social media site—the new age of electronics offers current employers even more insight. Current employers have access to their employees' electronic cache. It is rare to find any lawyer without a firm-issued smartphone and computer. Usually the firm also assigns an email address and provides the Internet access. These give access to information and activities that are not volunteered by the employee. For example, an electronic file scan may catch an employee receiving and sending sexually explicit emails, creating a sexually hostile work environment, or disclosing privileged (and juicy) client communications via email to third party friends and family.

TO PROTECT THEMSELVES FROM MERITORIOUS CLAIMS, LAW FIRMS SHOULD SEEK TO DIMINISH THEIR EMPLOYEES' EXPECTATIONS OF PRIVACY

But there is a big difference between looking at something an employee voluntarily makes public and something obtained from the employee without their permission.

California courts have provided some guidance on what types of actions cross the line from appropriate supervision to invasion of an employee's right to privacy. If the line is crossed, the employer risks a claim for invasion of privacy against an employer based on two separate legal theories, one grounded on the California Constitution, and the other based on a common law tort of invasion of privacy. Morphed together, the two types of privacy claims turn on the nature of the intrusion upon the reasonable expectations of privacy, and the offensiveness or seriousness of the intrusion, including any justifications. This leads to an inevitable balancing of interests, the outcome of which is often decided on a case-by-case basis.

Law firms must answer to the law just like any other employer. To protect themselves from meritorious claims, law firms should seek to diminish their employees' expectations of privacy. This can be done by implementing and religiously following a "no expectation of privacy policy," in which a written statement clearly expressing the policy is given to and acknowledged by all of the employees, from lawyers to entry level staff. This statement should also be clearly posted in any areas where videotaping is done. Such a policy typically states that the employer routinely, and without any further notice to the employee, will monitor computer use; read emails, texts and Twitter updates; listen to voicemails; and review hidden videotaped surveillance. But beyond the implementation and acknowledgement of such a policy, the facts in a particular case always carry ponderous weight on whether the employee has a reasonable expectation of privacy.

Emails

Regarding emails, the reasonable expectation of privacy can depend on whether the employee used a company computer, the company's Internet service provider, a company-issued email address, and a secret password to transmit and receive their emails. In *Holmes v. Petrovich Dev. Co.* (2011) 191 Cal.App.4th 1047, the plaintiff sent emails to her attorney regarding a possible legal action against her employer. The employer obtained the emails from her computer: the plaintiff demanded them back claiming that they were attorney-client privileged communications, and

sued the employer for invasion of privacy. The court held that the emails did not constitute "confidential communication between client and lawyer" within the meaning of Evidence Code section 952 because the plaintiff used the employer's computer to send the emails despite the facts that she had been told of the company's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal email. She had been warned that the company would monitor its computers for compliance with this company policy and thus might "inspect all files and messages ... at any time;" and she had been explicitly advised that employees using company computers to create or maintain personal information or messages "have no right of privacy with respect to that information or message." The court stated:

> When Holmes emailed her attorney, she did not use her home computer to which some unknown persons involved in the delivery, facilitation, or storage may have access. Had she done so, that would have been a privileged communication unless Holmes allowed others to have access to her emails and disclosed their content. Instead, she used the defendants' computer, after being expressly advised this was a means that was not private and was accessible by Petrovich, the very person about whom Holmes contacted her lawyer and whom Holmes sued. This is akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by Petrovich would be privileged.

The *Holmes* court distinguished *Stengart v. Loving Care Agency, Inc.* (2010) 201 N.J. 300, 990 A.2d 650, 659, 663–664, in which that court found that the employee had a reasonable expectation of privacy in the use of a personal Web-based email account—even though accessed from the employer's computer—where the use of such an account was not clearly covered by the company's policy and the emails contained a standard hallmark warning that the communications were personal, confidential, attorney-client communications.

Video Surveillance

As to the covert videotaping of employees, the legality of this is anchored by two extremes: covert videotaping in open and accessible workplace areas, and videotaping in areas reserved for personal acts.

THERE IS A BIG DIFFERENCE BETWEEN LOOKING AT SOMETHING AN EMPLOYEE VOLUNTARILY MAKES PUBLIC AND SOMETHING OBTAINED FROM THE EMPLOYEE WITHOUT THEIR PERMISSION

Videotaping in open and accessible workplace areas can be lawful. For example, the lobby and hallways of our firm electronically monitor the comings and goings of patrons and employees for security purposes. That is lawful. However, videotaping areas reserved for personal acts, such as employee restrooms, is unlawful. Indeed, there is little justification in any law firm, or any other company, that would override the right and expectation of privacy in such a personal area.

The outcome in situations that fall somewhere in between videotaping in open and accessible workplace ares, and videotaping in areas reserved for personal acts, are factually driven. For example, our computer server room, which is locked and accessible only by a few people in the firm, has electronic surveillance all the time. It is only actually monitored a few times a day, or when a high heat sensor, or a water intrusion alarm is triggered. This is a rational, reasonable intrusion. Even so, the eye of the camera can catch unintended images, and so the best practice is to always make a clear disclosure that electronic surveillance is taking place, even if the surveillance is for a rational, lawful purpose.

In *Hernandez v. Hillsides Inc.* (2009) 47 Cal.4th 272, the defendants operated a private, nonprofit residential facility for neglected and abused children, including

the victims of sexual abuse. Plaintiffs were emploees of the defendants. The plaintiffs shared an enclosed office and performed clerical work during daytime business hours. Their office had a door that could be locked, with blinds that could be drawn, and the plaintiffs could perform grooming or hygiene activities or conduct personal converations, during the workday in that office. The director of the facility, learned that late at night, after the plaintiffs had left the premises, an unknown person had repeatedly used a computer in the plaintiffs' office to access the Internet and view pornographic Web sites. Such use conflicted with company policy and with the defendants' aim of providing a safe haven for the children.

RIGHT TO PRIVACY CASES TURN ON WHETHER THE EMPLOYEE HAD A REASONABLE EXPECTATION OF PRIVACY UNDER THE CIRCUMSTANCES

Concerned that the culprit might be a staff member who worked with the children, and without notifying the plaintiffs, the defendants set up a hidden camera in the plaintiffs' office. The camera could be made operable from a remote location, at any time of day or night, to permit either live viewing or videotaping of activities around the targeted workstation. It is undisputed that the camera was not operated for either of these purposes during business hours, and, as a consequence, the plaintiffs' activities in the office were not viewed or recorded by means of the surveillance system. The defendants did not expect or intend to catch the plaintiffs on tape.

After discovering the hidden camera in their office, the plaintiffs sued the defendants, for, among other things, violation of their privacy rights under the California Constitution. The California Supreme Court reversed the Court of Appeal, and reinstituted the trial court's order granting the defendants' motion for summary judgment. The Supreme Court stated:

> We appreciate plaintiffs' dismay over the discovery of video equipment—small, blinking, and hot to the touch—that their employer had hidden among their personal effects in an office that was reasonably secluded from public access and view. Nothing we say here is meant to encourage such surveillance measures, particularly in the absence of adequate notice to persons within camera range that their actions may be viewed and taped.
>
> Nevertheless, considering all the relevant circumstances, plaintiffs have not established, and cannot reasonably expect to establish, that the particular conduct of the defendants that is challenged in this case was highly offensive and constituted an egregious violation of prevailing social norms. We reach this conclusion from the standpoint of a reasonable person based on defendants' vigorous efforts to avoid intruding on plaintiffs' visual privacy altogether. Activation of the surveillance system was narrowly tailored in place, time, and scope, and was prompted by legitimate business concerns. Plaintiffs were not at risk of being monitored or recorded during regular work hours and were never actually caught on camera or videotape.

In *Carter v. County of Los Angeles* (C.D.Cal 2011), 770 F.Supp.2d 1042, a case involving government employees (who have greater expectations of privacy from their government employers), the employer received an anonymous complaint alleging that a plaitiff employee, had engaged in sexual activity with a visitor in the dispatch room while she was on duty at night. The employer then installed a hidden video camera in a fake smoke detector in the dispatch room, and set it to record continuously, every hour of every day. The camera recorded several incidences of the act. One of the plaintiffs discovered the hidden camera a few months after it was installed and she (and other employees) sued her employer for, among other things, violation of her privacy rights under the California Constitution. In assessing the reasonableness of the plaintiffs' privacy expectations, the court noted that

the dispatch room door remained closed during regular business hours, non-dispatcher employees would typically knock before entering, and no one could see into the dispatch room. Furthermore, after regular business hours, it was not uncommon for plaintiffs to work alone in the room. The court concluded that the plaintiffs had a reasonable expectation of privacy in the dispatch room.

In assessing whether the surveillance was a sufficiently serious intrusion as to constitute an egregious breach of social norms, the court noted that the plaintiffs were recorded while they unknowingly performed private acts, the surveillance was constant, and it continued even after the stated objective was complete. The defendant monitored all of the employees, not just the subject plaintiff. Finally, there were several less intrusive methods available to the defendants in investigating the allegations against the plaintiff employee, but the defendants did not utilize them. Thus, the court held that the defendants violated the plaintiffs' right to privacy under the California Constitution.

The Bottom Line

Right to privacy cases turn on whether the employee had a reasonable expectation of privacy under the circumstances. The employer has ty to somewhat manage the risk of a claim of a violation of privacy and an adverse result by minimizing the employee's reasonable expectation of privacy. The employer should disclose to the employee that the employee is being observed and monitored, and how that is being done.

Mark S. Adams *focuses his practice on business litigation, including, contracts, products liability, corporate and partnership disputes, and hospitality litigation. He has wide-ranging trial experience in commercial disputes, including complex multi-party litigation and class actions. He has tried numerous cases in state courts, federal courts, and in domestic and international arbitrations. Mark's trial wins have been covered by Forbes, Reuters, Life Science Weekly and other publications. He has obtained two of California's annual 50 largest jury verdicts in the same year. Mark has taken or defended nearly 1,000 depositions throughout North America, Europe and the Middle East. He has been quoted as an expert on non-compete agreements in the Wall Street Journal.*

This article is available as a complimentary online self-study CLE article for members of the Law Practice Management & Technology Section.

Visit the members' only area at http://members.calbar.ca.gov/sections/lpmt for your coupon code and instructions on how to access the online self-study articles.

HOW TO RECEIVE MCLE SELF STUDY CREDIT

After reading this MCLE credit article, complete the test online at:

http://members.calbar.ca.gov/sections/lpmt

to receive 1.00 hour of MCLE self study credit.

FROM THE CHAIR

Will Hoffman

"Protection of the public" has been the mantra around the State Bar for the last several months. Because the legislature doubted the Board of Governors' ("BOG") dedication to that fundamental purpose, restructuring the BOG, or even the unitary State Bar itself, has been the hot topic. By the time you read this column, the changes proposed and disputed should be resolved—for this year at least. But the need to serve and protect the public is more than the slogan of the day.

To our LPMT Section, competent and ethical representation is, in and of itself, the substance of protecting the public and promoting justice and the public interest. Often ignored, however, is that doing well, however each of us defines it, is what allows most of us to do good. Hence, being able to develop and manage a thriving practice is often the sine qua non of effectively serving the public. LPMT endeavors to enable each of its members to build a successful practice, whatever the chosen substantive area(s). LPMT does so by helping each member build and maintain that healthy practice, whether in the context of a traditional firm, an in-house legal department, a government entity, or a public interest nonprofit. If the practice does not function well, success and satisfaction will elude both lawyers and clients.

BEING ABLE TO DEVELOP AND MANAGE A THRIVING PRACTICE IS OFTEN THE SINE QUA NON OF EFFECTIVELY SERVING THE PUBLIC

As Section members, we can all take pride in LPMT's deep reservoir of talent, knowledge, experience, and goodwill. Our Section contains tech wizards, deal-makers, paralegals, in-house counsel, bet-the-company-case litigators, legal secretaries, criminal-defense attorneys, professors, law librarians, and practice management gurus, to name but a few.

The LPMT Executive Committee mirrors this diversity. In addition to our official voting members, we appoint a set of Special Advisors. Among other benefits, when the State Bar wants to change the game, we're not caught flat-footed but rather can, and do, have the knowledge and experience to speak up for the best interests of California lawyers based on our broad knowledge of what most lawyers need to thrive.

LPMT's Special Advisors include our law practice management brain trust of Andrew Elowitt, Gideon Grunfeld, Larry Meyer, Ed Poll, and Neil Quateman. This year we have also elevated long-time LPMT Executive Committee stars Christèle Demuro and Yvonne Waldron-Robinson. The incomparable Robert Brownstone rounds out the group as Immediate Past Chair.

Looking forward

I invite your suggestions and recommendations on how LPMT can help you and the wider community. Let us know how LPMT can increase our value to you and your colleagues. Among other initiatives for the coming year, we will expand the number and variety of educational programs available. What would you like to learn? What would you like to teach? LPMT can set you up with a Webinar and promote it, at no cost.

Let's expand LPMT membership so that we can be of greater service. Recommend us to your colleagues. In addition, all California law school students are entitled to a free membership in LPMT. If you know one who has yet to join, tell her or him to email us with contact information, school name, and class year at LPMT@calbar.ca.gov.

California leads the world in both business and social innovation. We should match that spirit in how we structure our relationships with clients—and each other. Technology facilitates these new ways of being, but so does an evolving consciousness of who we are and how life should be lived, at work, rest and play.

While the BOG argues over the future shape of the board, LPMT will focus on the future shape of lawyering. Fewer and fewer lawyers do all of their work in a typical office, on a conventional schedule, marking time in fractions of an hour. Let us explore alternatives to both the nature of how one works and how one gets paid—crucial building blocks to excellent service to our clients and overall protection of the public.

Will Hoffman
2011-12 Chair
Law Practice Management & Technology Section
LPMT@calbar.ca.gov

Contact *The Bottom Line* at

thebottomline@calbar.ca.gov

STRUCTURING COMPENSATION FOR A COMPETITIVE MARKETPLACE

By Ed Poll

Ed Poll

During the past four years there has been more change and controversy regarding lawyer compensation than in the several decades before. Consider these key signposts on what has been a very bumpy and uncertain road:

- As the economy began its slide into recession, starting associate salaries of $160,000 and partners with $1,000 an hour billing rates were the talk of the law profession.
- Within two years, starting associate salaries at the largest firms were cut by 25 to 50 percent, and those associates still being hired were assigned to pro bono or internal internships.
- At the same time, senior partners viewed as not pulling their weight (that is, not bringing in enough billings to justify their high compensation) were de-equitized out of their firms.
- Offshoring of routine legal work to India and other countries, with a resulting cost savings of up to 80 percent over domestic lawyer rates, quickly became accepted…
- … only to be followed today by "onshoring" of the same work back to the U.S., to contract lawyers paid $50,000 and located in low-cost states like West Virginia and North Dakota.
- New virtual organizations like Axiom pay discounted rates to a freelance group of lawyers who used to work at major firms, but now work at home or at client locations.

Such developments reinforce the fact that law firms no longer can or will pay compensation out of scale with what clients will accept. There is a direct interrelationship between law firm billings, profits, and partner compensation. That interrelationship is expressed in various ratios and weightings, with wild cards like origination credits tossed in for good measure. But the essential fact is that the value clients want increasingly determines what lawyers will be paid. As embodied especially in the Association of Corporate Counsel (ACC) Value Challenge, that means more efficiency in fees, and less emphasis on increased profits per partner. The objective is lower costs, and law firms will increasingly feel the brunt of that effort.

Traditional Compensation Approaches

In such an environment, an understanding of how law firms arrive at lawyer compensation is essential. Typically there are considered to be two general compensation models: lockstep, in which the firm's overall success each year is averaged out to determine a standard rate of compensation increase for most lawyers, and "eat what you kill (EWYK)," in which all attorneys are rewarded on how much business they personally bring in. Each has advantages and disadvantages:

- Lockstep is good at building collaboration, client service teams, and institutionalizing clients.
- Lockstep is bad at rewarding exceptional performers and penalizing subpar performers.
- EWYK is good at developing new business and new markets, and spurring entrepreneurship.
- EWYK is bad at cross-selling services and promoting firm harmony.

Any firm that encourages lawyers to maximize their individual compensation may have

fast near-term growth. Approaching compensation as an institution makes for greater firm harmony and longevity. Either way, however, both lockstep and EWYK systems generally depend upon the same metrics: hours worked per year, origination credit, supervision credit, and other formulaic measures based on the billable hour. How many hours are billed *and collected* is the essential issue. The level of collections determines firm profitability, and profitability determines how much is available for compensation. The firm can either assess revenue to figure out what the cost structure should be so that the firm can turn a profit, or it can look at costs and determine how much revenue is needed to cover the costs and make a profit. These two models define what's available for the total compensation pool.

Law firms mirror their clients. To the extent that law firms provide the service their clients need, at the price clients are willing to pay, they will have an adequate compensation pool. Otherwise, they will be challenged to stay in business. As corporate clients seek to reduce their legal expenses by paring down outside counsel firms dramatically, the survivors are expected to provide certain work with relatively steady volume (such as patent filings or employment cases) at fixed rates over a certain period of time, turning these matters into the legal equivalent of a commodity. Commoditization is also increasingly becoming an issue for solos and small firms. The Internet has a growing list of legal services used by individuals (such as wills, bankruptcy filings, even divorces) being offered by law firms at low fixed prices.

Revenues Up, or Costs Down?

That brings us back to our two models for funding compensation: increasing revenues to cover costs, or reducing costs to match revenues. Begin with the revenue side. In a law firm, revenue is a highly personalized commodity because it is the product of each person's individual effort. The measure of that effort is billing rates and related fees, so increasing revenue puts the focus on whether to raise rates. Of course, in today's legal services environment, raising rates is generally a non-starter. Rates charged must be determined in the context of all the labor being devoted to client service, including paralegal and staff time as well as lawyer time. It is also possible to increase revenue by winning new business, but the chicken-or-egg issue here is whether the firm can do this if its rates are not low enough to be competitive.

LAW FIRMS NO LONGER CAN OR WILL PAY COMPENSATION OUT OF SCALE WITH WHAT CLIENTS WILL ACCEPT

The concerns on the cost side are no easier. Consider a law firm where the revenues from a given client are 10% less than the costs to service that client in lawyer and staff compensation. In this critical situation a decision must be made to reduce costs. The choices are hard, but each one must be considered in turn:

- Terminate the client relationship and the revenue it represents because the client cannot be adequately serviced within the firm's cost structure.
- Invest in technology for more efficient service, which may eventually reduce costs but in the near term raises costs due to the expense of equipment, software, and training.
- Assign fewer people to handle the client workload, which may decrease costs but also can decrease service to the point that the client is dissatisfied and pulls the business.
- Reduce staffing and leverage ratios so that lower-compensated associates and paralegals handle tasks formerly carried out by higher compensated senior partners.

It is apparent that there is no easy way to adjust costs to revenue. Certainly it can be done, but the strategies for doing it each have drawbacks that are hard to overcome.

The Team Solution

Given these complexities, the best compensation approach in today's cost-sensitive environment is a

variation on the lockstep concept: using the client team philosophy to both increase revenues and reduce costs. Base compensation in this approach is tied to the effectiveness of involving other firm lawyers as part of the team delivering legal services to clients. This allows for blended high and low rates on client work, maximizing revenue and profitability. Compensation is paid based on what is generated for the organization—not for any one individual—because the organization's revenue is maximized, and so too are profits, which are the lifeblood of organizational survival.

TO THE EXTENT THAT LAW FIRMS PROVIDE THE SERVICE THEIR CLIENTS NEED, AT THE PRICE CLIENTS ARE WILLING TO PAY, THEY WILL HAVE AN ADEQUATE COMPENSATION POOL

One can use a sports metaphor, comparing athletic teams that have one or two self-centered, freelancing stars to those teams with no stars, but great cooperative skills. While it is possible for the former to have a good season (often followed by a collapse), it is the latter model that is the more satisfying and longer lasting. The team model provides the greater satisfaction because the collective nature of the achievement allows everyone to stay at the top longer. The best law firm compensation approach gets away from a star system that rewards only the individuals who are out for themselves by also rewarding those individuals who help the team perform better. This creates a more profitable firm, from which all firm members benefit. In today's competitive legal marketplace, it enables billing, profits and compensation all to reinforce each other.

The team approach makes explicit the tie between individual compensation and the firm's overall revenue. Firms that service major clients with teams (not just a single rainmaker) can identify and provide needed practice specialties that reflect a full range of client concerns. A billing attorney coordinates the service provision according to a strategic plan, and can give clients a complete and virtually seamless service package. The client receives "one-stop shopping" from a group of lawyers who are chosen to address specific needs, both in terms of practice specialties as well as billing rates.

Teams represent a cooperative effort to increase revenue within a compensation model that depends on the success of the organization. Compensation is paid based on what is generated *for the organization*—not for any one individua—because the *organization's* revenue is maximized, and so too are profits, the lifeblood of organizational survival. In "The Business of Law®," as in the business of life, a rising tide does indeed lift all boats.

Ed Poll *is a speaker, author and board-approved coach to the legal profession. LawBiz® and Fujitsu are sponsoring Ed's cross-country tour to reach bar associations and law schools. If you want Ed to stop in your community, contact Ed directly. Readers with questions for Ed should email edpoll@lawbiz.com or call (800) 837-5880. You can also visit his interactive community for lawyers at www.LawBizForum.com.*

BUSINESS-TRAVEL SECURITY-HOLES AND HOW TO PLUG THEM

By Robert D. Brownstone

An oxygen-sucking hole ripped in an airplane's fusilage—though quite grave and potentially hazardous—is not the only leakage concern these days for business travelers. Thunderous voices, loose lips, wandering eyes, lost portable devices and aggressive customs officers are just some of the many circumstances that can compromise the confidentiality or privacy of information.

As a frequent traveler who also often advises clients and colleagues on information security and data leakage, I am hypersensitive—OK, call me just plain hyper. Over time, I have devised a series of routines to guard against disclosures of client confidences and identities, my law firm's proprietary secrets, and private information relating to me and my family. Hopefully, whatever your walk of life, you will find these ensuing tips instructive. Do try them at home.

As soon as you leave your office or home, security measures should kick in. The first rule of thumb is one I learned from the former prosecutors with whom I first practiced law in New York City, back in the pre-smartphone 1980's. They taught me about "location, location, location"; namely that, when, out in public, you should never mention names of companies or individuals represented by you or involved in any way in a confidential matter on which you are working. I distinctly remember one of my mentors Bill Purcell (a former Manhattan D.A.) reminding me to be careful each time we got into a cab to go to court or a deposition. Bill would calmly mention something to the effect that "you never know who will hop into the taxi next and strike up a conversation with our cabbie." Then, we would transition into "code name" mode. If we had to talk about a case, we would refer to key players as "Mr. C" or "Ms. M" and omit as many atmospheric and factual details as possible.

Once on the way to one's destination, in today's high-tech world people's loose-lips tendencies seem to have been exacerbated by ever-present cell phones—and even more so by the apparently requisite high volume of speech these cell phones require on a bus, train or plane. In the recent annals of publicly loud law firm partners, there are now such widely recognized characters as "Amtrak Bob" and "Acela Jim." Each of these men chatted noisily on a crowded train about a highly confidential personnel situation involving his respective law firm. According to news reports, Bob disclosed imminent layoffs that were not yet ready to be divulged and Jim called a young partner at another firm and recited the terms of an offer to try to entice the listener to jump ship and join Jim's firm.

Although the IT half of my persona wants to keep bashing lawyers, attorneys are not the only ones negligent in this regard. We've all experienced situations in an airport gate area or on a plane itself where we've heard a salesperson or an IT administrator revealing names, numbers, troubleshooting steps or other confidential details. "Speed kills": the ostensible need to talk to someone *that very instant* often trumps the risk of damage that could ensue from revealing a trade secret, the identity of a company with whom one is negotiating, or an inroad into a Web network.

In addition to big voices, the wandering eyes of others are a factor, too, especially on long, monotonous flights. Every task undertaken and every bit of information possessed on behalf of a customer/client warrants protection. Attorney-client privilege, the even broader ethical-duty-of-confidentiality, and all

Robert D. Brownstone

other lawyer and non-lawyer privacy obligations still apply at high altitudes. Thus, travelers should be especially careful about identifying customers or exposing other confidential information when using laptops on planes. A screen shield can prevent those to your left and right from looking at open items on your laptop. But I am used to employing a different process, just to play it safe . . .

Before I go to the airport, I rename any laptop folders and document names that bear client names, typically only keeping the first letter of the client's company name. If there are a lot of documents in a folder that I plan to access on the flight, I use Better File Rename software to anonymize or pseudonymise all pertinent file names. If I plan to edit a client-matter document that mentions a client name throughout, I run a *Ctrl+H* search-and-replace. Once I am back home or at my destination, it only takes another few clicks to undo those file-rename and search-and-replace temporary changes.

TRAVELERS SHOULD BE ESPECIALLY CAREFUL ABOUT IDENTIFYING CUSTOMERS OR EXPOSING OTHER CONFIDENTIAL INFORMATION WHEN USING LAPTOPS ON PLANES

Laptops (and, whenever possible, other portable devices), once encrypted, enable one to reap two major benefits, one altruistic and one selfish. First, the humane reward: in case the machine gets lost or stolen, whoever has the laptop will not be able to pull any data, let alone confidential information, off of the machine. As a result, confidential information as well as private information about co-workers, customers and others is protected. Second, the self-interest boon: anti-identity-theft statutes typically exempt lost or stolen *encrypted* personally identifiable information (PII) from triggering the duty of the data owner to give notice of breach. Thus, those who take precautions are spared the monetary costs and the PR-hit that inevitably follow a notice-of-breach scenario.

But even if encryption protects files from getting into other hands, one's work has been for naught if he or she didn't back-up a document to another location. So, after each flight, a best practice is to copy new or newly edited documents back to the law firm's network. Our firm's IT Director Kevin Moore trained me years ago that the hard drive of a portable computer or device is like cash, but central storage on a network is like a credit card. The former, if lost or stolen, is lost for good. The latter is recoverable even if one local copy of it is lost or corrupted.

Along those same lines, go paperless as much as possible. Consider taking a portable scanner and scanning all paper documents, receipts, handwritten notes that you create or gather on the trip. The scanner I use, the Visioneer Road Warrior, is about the same bulk as a light three-hole puncher. The only accoutrement it needs is a USB cable to attach to my laptop. As I find keeping track of physical objects increasingly distracting, I don't want to worry that I might have dropped —or left in the hotel room—a receipt or some notes or a prospective client's business card. Once scanned and saved to my work network, each item is safe, secure and backed up. For business cards in particular, specialized user-friendly scanning software enables easy conversion into an electronic contact that can be saved right into, for example, Microsoft Outlook or a webmail contacts list.

Assuming one has been careful en route, what of the urge to surf the Web on a big screen during down time at a hotel lobby or café computer? If you do check e-mail over a browser on a public computer, presumably you are not logging into a work email system via, for example, Outlook Web Access. If, however, you feel you must check work mail (or a personal Webmail account inbox) in this fashion, then at least make sure not to save the login or password or to download any confidential files.

On one cross-country trip, while waiting to deliver a workplace information-security presentation, I checked my personal Yahoo Webmail on a hotel registration-desk PC. Once I had deleted the browser history and then closed the browsing window, I happened to notice something on the desktop; it was called "[REDACTED FIRST AND LAST NAME]_Severance.doc". As soon

 CONTINUED FROM PAGE 12

as I hovered on the file's icon, a yellow rectangular bubble appeared, displaying the company name and the first name of the original "Author" of the document —or of its parent or grandparent document (according to some studies, 90% of electronic documents are created by editing a pre-existing document.) By right-clicking on the icon and then glancing at the "Properties" of the document, I was readily able to ascertain the original "Title" of the document. That Title reflected a *different* first and last name than that of the individual who was apparently about to be terminated via the current iteration of the document.

Without even opening the file, basic metadata allowed me to learn a fair amount of confidential information that was not meant to become public. I did delete the file and then emptied the recycle bin, such that only a computer forensics expert would have been able to resurrect the document from that machine. I have never disclosed—and long since forgotten—the names I had stumbled upon, but the impact of that experience brought home to me how much more dangerous it is to lose a stray electronic document somewhere virtual than to leave a relatively one-dimensional piece of paper in a physical location. In the twenty-first century, inevitable human error can have much broader ramifications due to the many layers of information available in an electronic file.

Let's presuppose you made it through your trip without incident, physically and digitally. Now, what about the return trip home? If you travelled outside of the United States, hopefully you took special care at the beginning of your trip. Why? Under current Fourth Amendment law, upon anyone's return to the U.S. from overseas, the contents of his or her laptop—or other digital device—are subject to warrantless inspection at the discretion of customs officials. No particularized suspicion of wrongdoing is required. Some courts have even ruled that a password or an encryption/decryption key must be disclosed upon request.

Just last month, yet another federal appellate decision came down supporting the legality of warrantless border searches of laptop computers. So, what is a business traveler do? A multi-pronged work-around could be: use a loaner laptop that houses neither a full set of company-provided computer programs nor any confidential files/data; throughout the overseas trip only do sensitive work over the Internet via a virtual private network (VPN) connection; store no newly created or modified confidential files on the local hard drive; and, before the return flight home, run an application such as powerful freeware tool CCleaner to "wipe" the hard drive.

Whether at home in your day-to-day routine or out on the road, always be circumspect about which information you choose to store on a portable computer or device. When in doubt, leave information in secure central storage that you can access remotely in a location-independent fashion. In general, remember the wisdom of the old "Hill Street Blues" Desk Sergeant Phil Esterhaus, who always urged his minions: "Let's be careful out there."

Robert D. Brownstone *is the Technology & eDiscovery Counsel and the Co-Chair of the Electronic Information Management (EIM) Group at Fenwick & West LLP, a 300-attorney Silicon-Valley-headquartered law firm specializing in representing prominent high-technology and life-sciences companies. Known as "Law & Technology in One Brain" or "The Guru of Metadata," Mr. Brownstone is a nationwide advisor, presenter and writer on many law-and-technology issues, including privacy and information-security. He is often quoted in the press as an expert on electronic information and teaches eDiscovery Law & Process at two law schools. Mr. Brownstone can be reached at rbrownstone@fenwick.com or (650) 335-7912.*

THIS ARTICLE DOES NOT CONTAIN LEGAL ADVICE.

THE IMPENDING COLLISION OF "FREE TO THE PUBLIC CLOUD STORAGE" AND EDISCOVERY

By Bill Tolson

Bill Tolson

The discovery process is tough, time consuming and expensive. In many cases, the electronically stored information ("ESI") collection process has become a frustrating game of hide and seek. Adding to this frustrating process, corporate attorneys are now facing the possibility of custodians storing corporate ESI up into "free to the public cloud storage" services, in many cases without the knowledge or approval of the organization's legal or IT department.

Cloud computing and cloud storage are an important capability that most organizations will embrace. This article is not a commentary on IT-supervised cloud storage but rather those cloud storage services that are being offered by companies like DropBox, Amazon, Apple and Microsoft to individuals for free. First, what is "free to the public cloud storage"? For the purposes of this article I will define it as a minimum amount of storage capacity offered by a third party, stored and accessible via the Internet and made available to the public at no cost (with the hope you purchase more). These cloud storage offerings do not limit the types of files you can upload to these services. Music storage is a prime target for these services but many, like me, are using them for storage of other types of files such as work files, which can then be accessed and used with nothing more than a computer and Internet connection, at anytime from anywhere. (See Figure 1)

As I mentioned above, examples of these "free to the public cloud storage" offerings include Dropbox (http://www.dropbox.com/), Amazon Cloud Drive (https://www.amazon.com/clouddrive/learnmore), Apple iCloud (http://www.apple.com/icloud/), and Microsoft SkyDrive (https://skydrive.live.com/). The danger of these types of services is that employees can create accounts without the knowledge of IT or the legal department and use them to store all types of company-related files. These files then exist outside the capability of the company to find them for eDiscovery response or regulatory production. As I will describe later, this practice will raise the cost and risk of the eDiscovery process for companies whose employees who use these services.

How prevalent are these services? Dropbox has reported more than 25 million users with an estimated 300 + million files stored.

Service	Free Storage
Dropbox	2 GB
Amazon Cloud Drive	5 GB
Apple iCloud	5 GB
Microsoft SkyDrive	25 GB

The differences between the four offerings stem from the amount of free capacity available at sign up and how you access your files. For example, on the next page is the Amazon Cloud Drive Web interface. (See Figure 2)

The advantage of these cloud storage services is the ability to move and store work files that are immediately available to you from any location, from any computer. This means you no longer have to copy files to a USB stick or worse, email work files as an attachment to your personal email account. The most obvious disadvantage of these services is that corporate information can easily migrate away from the security of the company infrastructure. Another risk is your company's ESI will be in the hands of a third party with whom your organization has no

agreement or understanding with respect to how the third party will respond to eDiscovery requests. These new public cloud storage offerings all boil down to rising risk and cost of discovery for corporate legal, and a new location to discover for opposing counsel.

To complicate the situation further, even deleted ESI is not really removed completely. In a recent blog post (http://ediscovery101.net/2011/05/16/is-the-popular-dropbox-file-sharing-application-a-huge-ediscovery-risk/) I talked about the public cloud storage service called Dropbox. Dropbox has a "feature" of not completely removing ESI when deleted from their application. Dropbox also keeps a running audit log of all interactions of the account (all discoverable information). The Amazon Cloud Drive has the same "feature" with the deletion of files. For example after deleting a file in the Amazon Cloud Drive, you must go into the deleted items folder of the service and "permanently" delete the file (See figure 3).

An important question to address is how corporate counsel, employees and opposing counsel will address this new potential target for responsive ESI collection? Take, for example, a company that doesn't know of the possibility of public cloud storage as a potential litigation hold target, doesn't ask employees about their use of these services, and doesn't search these accounts for responsive ESI. This potential spoliation condition will become more of a risk as employees discover these new services and organizations don't put policies in place to stop or at least control them inside the organization's firewall.

Points to be aware of with "free to the public cloud storage":

For Corporate Counsel:

1. Be aware that these types of possible ESI storage locations exist. No doubt opposing counsel will.
2. Create a use policy addressing these services. Either forbid employees from setting up and using these services from any work location and company equipment or if allowed be sure employees acknowledge that these accounts can and will be subject to eDiscovery search.
3. Audit the usage policy to insure it is being followed.
4. Enforce the policy if employees are not following it.

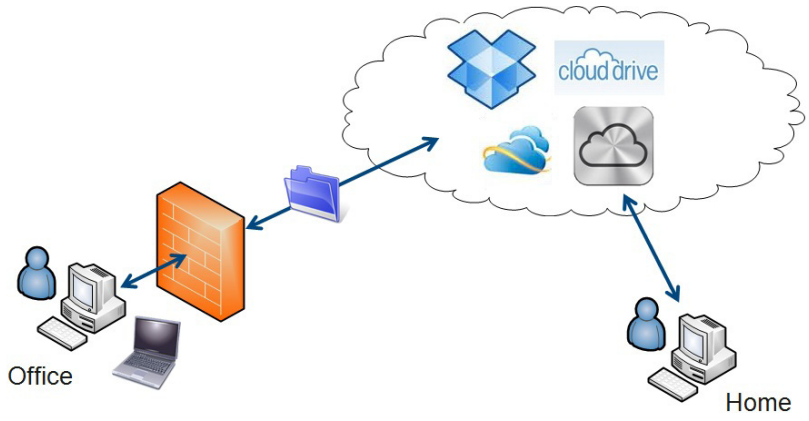

Figure 1: There is little stopping employees from utilizing "free to the public cloud storage" from their office locations.

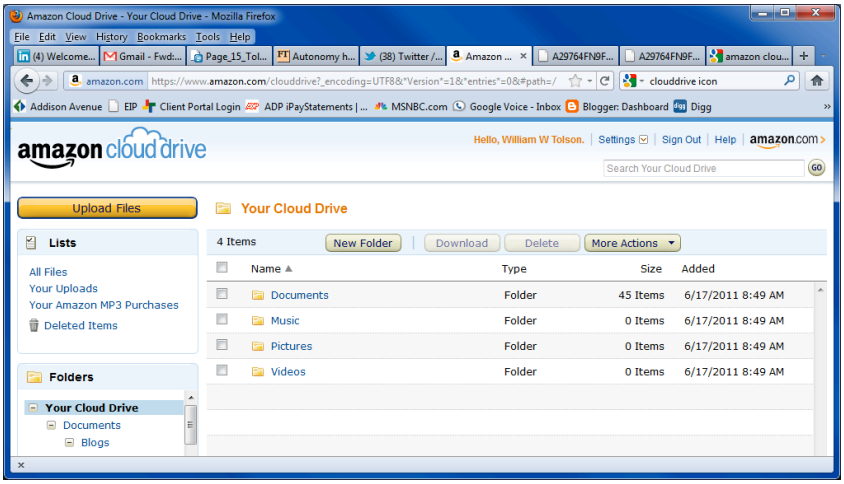

Figure 2: The Amazon Cloud Drive Web interface.

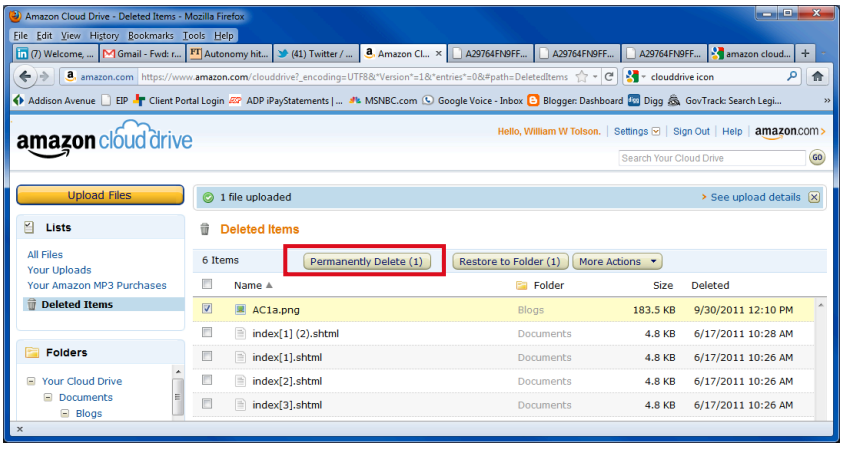

Figure 3: The deleted items folder in the Amazon Cloud Drive actually keeps the deleted files for some period of time unless they are marked and "Permanently Deleted.

 CONTINUED FROM PAGE 15

5. If allowed, create ESI retention polices specifically for these storage locations, audit employees to insure the retention policy is being followed, and enforce punishment if the policies are not being followed.
6. Document everything.

For Employees:

1. Understand that if you setup and use these services from employer locations and equipment and with company ESI, all ESI in that account could be subject to eDiscovery review.
2. If you use these services for work (and you have been given approval), only use them with company ESI, not personal files.
3. Be forthcoming with any legal questioning about the existence of these services you use.
4. Don't download any company ESI from these services to any personal computer. This could potentially open up that personal computer to eDiscovery by corporate counsel.

Opposing counsel should ask the following questions to the party being discovered (a Greenfield opportunity):

1. Do any of your employees utilize company sanctioned or non-sanctioned public cloud storage services?
2. Do you have a use policy that addresses these services?
3. Does the policy penalize employees for not following this use policy?
4. Do you audit this use policy?
5. Have you documented the above?
6. In responding to this discovery request, did you search all public cloud storage locations where potentially responsive ESI could have been stored?

These public cloud storage services are an obvious path for employees to utilize over the next couple of years to simplify their work lives. However, all parties involved need to be aware of the eDiscovery implications. As mentioned at the beginning of this article, cloud storage is a viable and useful service for organizations of all sizes. It relieves the organization from having to continuously purchase new storage assets while also serving as a best practice disaster recovery capability.

Don't dismiss cloud storage; just control it.

Bill Tolson *is a vetren of the computer storage and eDiscovery/Litigation support industry with more than 20 years experience. Previously, Bill was a principal consultant and practice manager for Contoural Inc. where he led the eDiscovery and compliance consulting business specializing in storage solutions, email archiving, enterprise content management, and information lifecycle management. Bill is the author of two eBooks* the Know IT All's Guide to eDiscovery *and* The Bartenders Guide to eDiscovery *and co-author of the book* Email Archiving for Dummies. *Bill has been a featured speaker at many legal and archiving events including the AIIM 2009, ARMA, ARMA Canada, LegalTech West, Storage Networking World, the IT Summit, and TechTarget's Email Archiving Series. Bill has held senior management positions at Hewlett-Packard, Hitachi Data Systems, StorageTek, and Iomega.*

PRIVACY BY DESIGN: BUILDING PRIVACY INTO THE ARCHITECTURE OF PRODUCTS AND SERVICES

By Mari J. Frank

Mari J. Frank

Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies, systems, products and services. This approach originally had information technology as its primary area of application, but has since expanded its scope to include business practices and physical design and infrastructures. Mari Frank recently discussed *Privacy by Design* with its original developer, Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian.

Frank: *Tell us the basics about Privacy by Design.*

Cavoukian: Let me just set the stage. Up until now, generally speaking, privacy was protected through various laws, regulations and policies. The problem is, this works in what I call the "old world," where we had lots of time to develop policies and procedures. It was a slower world.

Fast forward—we have online social media growing at unbelievable paces; we have over 600 million users on Facebook, everyone's on Twitter, you have geo-location data everywhere, everyone has mobile communications, cell phones, Wi-Fi everywhere. Everything is now working into the Cloud, you have Cloud Computing, Web 2.0, Web 3.0—so the world is accelerating at such a pace that the changes that we've experienced in the last five years have out-paced all of the changes in the preceding fifty years, which were themselves considered remarkable.

Given that backdrop, how can you expect to protect privacy, in this new world, in the same way we've been doing it for the past hundred years? We need a different way; the different way I'm suggesting is *Privacy by Design*. The distinction is this: the existing order relies on a regulatory screening scheme where some harm takes place, some privacy infraction; then, someone complains to a regulator, like myself. I investigate and then I provide them with some form of redress. It's all sort of a *harms based approach* that requires someone to come forward and someone who investigates, and it's a lengthy process even when we move quickly. In that model, I know as a regulator that I only see the tip of the iceberg. There are only so many people who come forward, there are only so many infractions that you're actually going to catch. The majority go unknown, unregulated, unchallenged. I don't want that. I want to change the paradigm; that's what *Privacy by Design* does. So what it tries to do is, it says to everybody—technology companies, businesses, governments, everyone—try to imbed privacy proactively, starting with technology. Imbed it in the design, the very architecture of technology; imbed it as core functionality, right from the outset, at the time the design specifications are drafted. So this is the basic shift in mindset to look at these things proactively. The goal is prevent the harm instead of trying to resolve it after the fact. And this is also, incidentally, much more cost efficient and more effective.

Frank: *What are the seven steps of Privacy by Design?*

Cavoukian: They're really simple; one might say they're obvious. The first principle is **be proactive, not reactive**. Try to prevent the harm instead of offer remediation after the fact.

Frank: *The old approach is "Let's get the technology and take care of privacy later."*

Cavoukian: And it doesn't work! Even

when they try to do it later, the retrofitting of the protections, the bolted on solution, is never as effective, and it costs more! That's how I get through to these utilities and companies. This is going to cost you less; it's going to save you money in the future.

Second principle, very simple: **privacy as the default setting.** This is the hardest principle because by default I mean it's the condition that happens automatically, you don't have to ask for it, it's there.

Third one is **privacy imbedded in design,** the very architecture of the system. The fourth one is very important; I don't want people to lose sight of this one. It's called **full-functionality, positive sum not zero sum.** We all know a lot about zero sum; it's either/or, it's the balancing act. You can have this *or* you can have that. Rarely the two shall meet.

Frank: *I've heard you talk about others saying, "You can have privacy or security." And that's just not the case! You can have both privacy and security.*

Cavoukian: And that's what we call positive sum, meaning you can have two positive increments of two different interests of functionality. So I tell people, it's not privacy 'vs.' security, it is privacy *and* security. The fifth one is absolutely essential: **end to end security.** Again, privacy is not contrary to security; you cannot have privacy without strong security. Cybersecurity is absolutely essential. We call this full-life cycle protection.

Frank: *It's important for businesses that don't think hard about privacy to note that this means not only when you collect data, but when you are done with it as well.*

Cavoukian: Oh, I'm so glad you raised that—to have that last level of secure destruction is *absolutely* critical.

Frank: *And do many businesses forget about that?*

Cavoukian: Yes, it's just off their radar. The sixth principle is **visibility and transparency**; keep it open. If you remain visible, in terms of your information practices (what are you doing with the information, how are you using it, who you're giving it to, more importantly, who are you *not* giving it to without their consent) customers will then be loyal, respect you and give you their repeat business. And the last one, **respect for user privacy**. If you focus on the user and as you're designing your systems and your processes, you stay focused on the user, it's easy! The rest of it falls into place, because then you've got respect for the user built throughout the whole system.

Frank: *Privacy by Design is a wonderful way to prevent privacy harms proactively instead of dealing with the tremendous costs and challenges of trying to resolve the problems after the fact.*

Mari J. Frank, *Esq. CIPP, is an Attorney and Privacy Mediator, and a member of the Executive Committee of the Law Practice Management Section of the State Bar. Since 2005, she has been the host of "Privacy Piracy" a public affairs radio program at the University of California, Irvine, dedicated to privacy issues in the information age. Ms. Frank recently talked to Dr. Ann Cavoukian, Privacy Commissioner of Ontario, Canada, about how companies and law firms can benefit from Privacy by Design. The following is a short excerpt from Ms. Frank's interview with Dr. Cavoukian. The entire interview can be accessed at www.kuci.org/privacypiracy or on iTunes. Ms. Frank can be reached at www.identitytheft.org or Mari@marifrank.com.*

ARBITRATION OR THE CODE OF CIVIL PROCEDURE: WHICH IS MORE LIKELY TO BAR YOUR CLAIM?

By Adam D. H. Grant

Adam D. H. Grant

Should businesses insert an arbitration clause into their contracts with clients and enjoy the informality of such proceedings, or should they opt for the more formal procedures detailed in the Code of Civil Procedure? While the informality of arbitration is inviting, businesses could be giving up rights that may forever prevent a future-related claim.

Procedural rules in arbitration take precedence over the Code of Civil Procedure because that is what the parties agree to be bound by when they sign the contract. The parties understand that when they enter into such agreements, the procedures are less formalistic and more streamlined to permit an arbitrator to expeditiously dispose of the matter.

Consequently, the state Supreme Court has acknowledged that, while arbitration is relatively quick and inexpensive, it is somewhat roughshod, requiring the parties to accept the bad with the good. *Brennan v. Tremco Inc.* (2001) 25 Cal. 4th 310, 316. Wanting the efficiency and cost-effectiveness of private arbitration, many businesses choose to abide by a commonly used arbitration clause that requires parties to submit any claim or dispute to the American Arbitration Association and be governed by the then-existing AAA rules.

If a dispute arises and arbitration begins, AAA rules do not require a party to provide a formal response; if a party does not respond, the rules presume a general denial. Rule 4(b). The opposing party need not even appear at the hearing. Rather, with the moving party present, a "prove up" hearing will be conducted before the arbitrator and an award determined. The award will likely acknowledge the existence of the arbitration agreement, the proper notice of the hearing, the lack of appearance by the opposing party, the receipt of the necessary evidence, and the arbitrator's findings. The moving party will obtain a court order confirming the award. The losing party is then on the hook for the award.

At this point, to avoid enforcement of the judgment, the losing party may now go on the offensive and file a complaint on different, but related, issues to try and settle the entire dispute. Unfortunately, the roughshod procedure created in the AAA rules may chill the party's ability to assert these claims due to the doctrine of *res judicata*. Interestingly, the relaxed procedural nature of a private arbitration is what will lead to the losing party's demise. The more stringent requirements of the Code of Civil Procedure would have allowed the party to resurrect the claims.

WHEN DECIDING TO SUBMIT MATTERS TO ARBITRATION, EACH PARTY MUST WEIGH THE PERCEIVED COST SAVINGS AGAINST THE RELAXED PROCEDURAL REQUIREMENTS

The key in determining the application of *res judicata* is whether the opposing party's claims were "actually litigated." This doctrine bars "all grounds for recovery which could have been asserted, whether they were or not, in a prior suit between the same parties ... on the same cause of action, if the prior suit concluded in a final judgment on the merits." *International Union of Operating*

 CONTINUED FROM PAGE 19

Engineers-Employers Const. Industry Pension, Welfare and Training Trust Funds v. Karr, 994 F.2d 1426, 1429 (9th Cir. 1993.).

The state Supreme Court has been very clear that *res judicata* encompasses related matters that *could have been raised* even though not expressly pleaded or otherwise urged. *Sutphin v. Speik* (1940) 15 Cal. 2d 195.

If the parties chose to follow the Code of Civil Procedure, however, counter-claims are not "actually litigated." A change in Code of Civil Procedure Section 426.30 created this anomaly. This section permits a party to later plead a related claim, but only if the defendant in the first action did not file an answer.

Such is not the case when the parties agree to follow AAA rules. Under the AAA rules, all related claims are "actually litigated." In fact, Rule R-29, which governs commercial arbitration, specifically notes that an award "shall not be made solely on the default of a party." The arbitrator must require the complaining party to do an actual "prove up" hearing to justify the award. Thus, if the parties sign an agreement that specifically states the matter is to be governed by the AAA rules, Section 426.30 will not apply.

When deciding to submit matters to arbitration, each party must weigh the perceived cost savings against the relaxed procedural requirements. However, in doing so, a party must realize that it foregoes the procedural safeguards otherwise available by the Code of Civil Procedure. Without such safeguards, inaction may bar a claim that would not otherwise be barred.

Adam D.H. Grant *is a principal with the Encino law firm Alpert, Barr & Grant APLC and is a trustee for the San Fernando Valley Bar Association. His practice areas include complex business litigation, construction law, real estate and general liability claims. He can be reached at agrant@alpertbarr.com.*

THE *LAW PRACTICE MANAGEMENT & TECHNOLOGY SECTION OF THE STATE BAR* WOULD LIKE TO THANK THE FOLLOWING LEGAL SERVICES VENDORS WHO SPONSORED, IN PART, LPMT'S WELCOME RECEPTION AT THE STATE BAR ANNUAL MEETING ON SEPTEMBER 16, 2011:

Bay Area Legal Forum

Excellence Through Education

The ***Bay Area Legal Forum*** is dedicated to providing quality, continuing education for the legal community. Our members are comprised of legal secretaries, paralegals, attorneys, and court staff throughout the Bay Area, and meet approximately every six to eight weeks to plan our programs. The Forum presents quarterly single-subject workshops and annual seminars each April consisting of between 8 and 10 workshops. Our next quarterly workshop will be presented on October 29, 2011. For details on all of our programs visit our website at www.bayarealegalforum.org

ESI

Engineering and Scientific Investigation

Engineering Systems Inc. (ESI) is a national multi-disciplinary engineering and scientific investigation firm. We have offices in 10 states including California. ESI's technical disciplines include: Aeronautical, Automotive, Biomechanical, Civil, Electrical, Intellectual Property, Marine, Materials, Mechanical, Metallurgical and Structural Engineers. Please visit our website at www.esi-website.com.

First Legal | Investigations

2112 North Main St, Ste. 220, Santa Ana, CA 92706
www.firstlegalnetwork.com 866.882.5111
CA PI: 24171 AZ:1551710 NV PI–PS: 1452

First Legal Investigations is a U.S.-based full service licensed detective agency with offices strategically located throughout California, Nevada and Arizona. For over 27 years, our team of professional investigators has provided the highest level of service to our clients both domestically and internationally. We provide services to the legal profession, insurance industry, municipalities, large corporations and small businesses.

GLENN M. GELMAN & ASSOCIATES

BUSINESS ADVISORS

CERTIFIED PUBLIC ACCOUNTANTS

Glenn M. Gelman & Associates is distinguished as one of southern California's premier business valuation and litigation support firms. Our practice is devoted to providing attorneys and their clients with a diverse continuum of forensic accounting, business valuation and litigation support services. Our litigation support services include: Business Valuation, Forensic Accounting & Investigation, Litigation Support, Record Reconstruction, Economic Damages & Analysis, Expert Testimony, Trial Preparation & Settlement Negotiations, Asset Tracing, Preparation of Net Worth Statements, Enhanced Earnings Calculation, and Stock Option Valuation.

www.lsi.org

LSI – Educating California's Legal Professionals

Established in 1934, ***Legal Secretaries, Incorporated***, also known as "LSI", is a nonprofit mutual benefit corporation organized for the purpose of providing education and professional and personal development programs to its members. Membership is open to anyone within the legal profession. In addition to legal secretaries, the membership includes court clerks, court reporters, paralegals, legal assistants, legal administrators, banking/trust department personnel, and attorneys. LSI offers the only California Certified Legal Secretary® program in the state and membership in six Legal Specialization Sections. LSI is an approved MCLE provider. For more information about LSI, visit us at: www.lsi.org.

PARASEC
GLOBAL DOCUMENT FILING & RETRIEVAL

Filing and retrieving public records documents can be complex, time consuming, and requires "knowing the system" to get the right results. ***Parasec*** searches, files and retrieves public documents in all 50 states and manages the bureaucracy for an easier, faster and more reliable process. Parasec works with major law firms, Fortune 500 companies and entertainment firms nationwide and has nearly 35 years of nationwide experience in entity formations, registered agent services, title-research services, the Uniform Commercial Code, and more. With additions like an online MCLE viewer delivering all your necessary 25 credits for only $125 (CA), our new Paracorp Entity Manager platform, and our Internet Reputation Reporting for real time data-captures of internet data in an evidentiary format, we continue to deliver high levels of service at affordable prices. Let us know how we can help your practice today.

ProLegal
COURT • PROCESS • DELIVERY
ON-DEMAND AND ON-LINE LEGAL SUPPORT SERVICES

Pro Legal, a division of Pro Courier, is Southern California's premier attorney services firm. We specialize in on-demand and on-line Court Filings, Service of Process, Subpoenas, Same Day Delivery, Research, Messenger services and much more. To better serve you, we are open 24 hours a day, seven days a week and have over 500 employee-based drivers in Southern California alone. We take pride in our customer service, attention to detail, consistent on-time performance and clear communication between our clients and our employees. Due to our unique nature, we can customize any of our services to fit your firm's needs. We do not expect you to fit into our business model; we will fit into yours.

VERITEXT®
National Deposition & Litigation Services
BETTER IN EVERY CASE

Veritext is the premium provider of court reporting and litigation support services nationwide. We leverage our years of experience in the complex arenas of intellectual property, pharmaceutical and product liability, securities, commercial, employment and antitrust cases for many of America's largest corporations and law firms. For over a decade, Veritext has focused on developing innovative solutions to support litigation attorneys from discovery through trial. With Veritext's advanced technology in VIP21, Mobile Depo, Native Evidence Capture, Exhibit Management Solutions, and much more, we are able to reduce our clients' costs and increase productivity.

We solicit original manuscripts, which should be typed double-spaced in an 8-1/2 x 11 format and submitted via email in MS Word. Articles are limited to 1,250 to 2,500 words. Authors should provide sufficient information to permit adequate identification in the publication. The editorial staff reserves the right to edit submitted manuscripts as necessary. Edited manuscripts will be sent to authors for approval only where extensive revision might affect an article's substance. Strict publication deadlines do not allow time to send a proof to authors. Manuscripts should be sent to: LPMT c/o California State Bar via email as follows: kristina.robledo@calbar.ca.gov

In most cases, we can grant reprint permission to recognized professional organizations. Inquiries regarding subscriptions, etc., should be addressed to:

Kristina Robledo
State Bar of California
180 Howard Street
San Francisco, CA 94105-1639

Contact *The Bottom Line* at

thebottomline@calbar.ca.gov