BLF
BIGGER LAW FIRM
A magazine for attorneys

LAW + TECH

Facing the changing landscape of cloud security standards

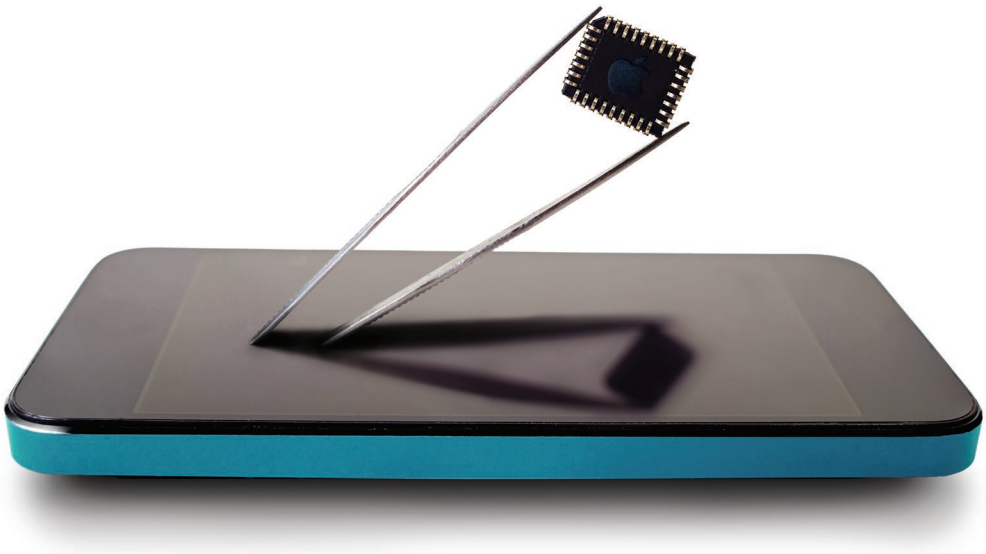
PRACTICE MANAGEMENT

Can enterprise social networking tools work for law firms?

GET SOCIAL

Social media governance: risk management and brand management for law firms

Inside



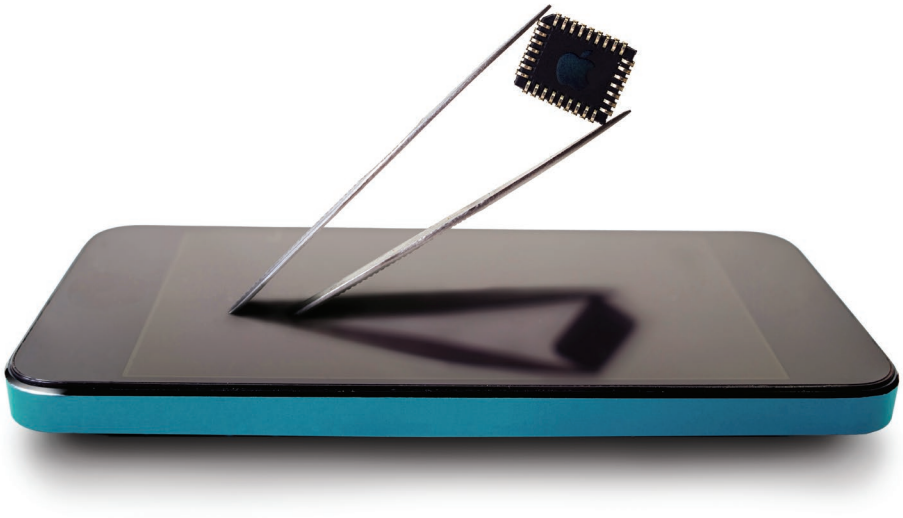
THE DIGITAL ARMS RACE: APPLE, THE FBI AND A LAW AGAINST SECRETS

ISSN 2163-2464
9 772163 246007 39 >

March/April | Vol. 39

FEATURES

BLF
Mar/Apr 2016



The Digital Arms Race: Apple, the FBI and a Law Against Secrets

The FBI has dropped its case against Apple. But the greater question of whether companies' and citizens' use of and access to strong cryptography will eventually be curtailed by the courts or by Congress still looms.

9

3

LAW + TECH

Meeting Changing Cloud Computing Security Standards

Attorneys have a responsibility to keep clients' confidential information secure, and cloud computing is of particular concern in this regard.

14

GET SOCIAL

Social Media Governance

The widespread attraction of social media for individuals as well as firms has the potential to both enhance and disrupt the ways people interact and firms grow. An effective social media policy should aim to generate a competitive advantage while diminishing loss.

BLF BIGGER LAW FIRM
A magazine for attorneys

Bigger Law Firm™ was founded to introduce lawyers to new marketing and firm management ideas. Advancing technology is helping law firms cover more territory, expand with less overhead and advertise with smaller budgets. So many tools exist, but if attorneys are not aware of these resources, they cannot integrate them into their practice. The *Bigger Law Firm* magazine is written by experienced legal marketing professionals who work with lawyers every day. This publication is just one more way Custom Legal Marketing™ is helping attorneys Build a Bigger Law Firm™.

To send mail to this publication, write to Adviatech Corp., *BLF* magazine, 4023 Kennett Pike Suite 57516 Wilmington, DE 19807, or email editor@biggerlawfirm.com.

Editor	Cristina Fries
Art Director	Kristen Friend
Staff Designer	Laura Donnell
Staff Contributors	Brendan Conley, Ryan Conley, Kristen Friend, Roxanne Minott, Dipal Parmar, Kerrie Spencer
Subscriptions	Thomas Johnson, tjohnson@biggerlawfirm.com
Founder	Jason Bland
Website Offers	www.biggerlawfirm.com
Single Issue	$6.95

SEO OBITER DICTA

The Reports of SEO's Death Are Greatly Exaggerated

Since 1997, bloggers, "experts" and internet pundits have been declaring that SEO (search engine optimization) is dead. In April 2015, *Entrepreneur Magazine* published a piece titled "The Top 4 Reasons SEO is Dead." In December 2016, Lexis Nexis' Business of Law Blog reiterated the sentiment in their article titled "6 Bold Predictions for Legal Marketing in 2016" wherein number 1 was "End of the road for SEO."

What happened? Let's explore the reasoning behind these morbid predictions.

The *Entrepreneur* piece points out that Organic Reach is down, citing websites like Yelp and Facebook as claiming marketshare in consumer decisions. While review sites and social networks definitely play into consumer decision making, organic reach for law firms is not down, the audience is just behaving differently.

If you look at Google Trends for terms like "lawyer" or "attorney," you will see what looks like a subtle downward trend between 2004 and today. But look at "lawyer near me" and you see significant growth since 2013.

Get more specific with searches like "car accident lawyer" and you see subtle growth since 2004. Compare that to "car accident lawyer near me" and the trend is in line with the generic "lawyer near me" growth that started in 2013.

We also look at conversational keyphrases like "I need a lawyer." That keyphrase has quadrupled since its 2006 lows. While there is no denying the point that traffic is becoming less centralized and review sites along with social networks claim consumer marketshare, organic reach for lawyers is certainly not down.

Let's examine LexisNexis' Business of Law Blog's claim that 2016 is the "end of the road for SEO." The full quote states, "SEO officially becomes obsolete in 2016, killed off by repeated Google artificial intelligence and algorithm updates."

Google has certainly gotten smarter, and as we covered in December 2015's Bigger Law Firm Magazine article, "Google's Rankbrain and the Future of Smart Search," Google's algorithm aspires to learn. And it's no secret that since Google's 2003 update titled "Florida," they have aggressively been shaping their algorithm to sniff out and demote websites that have so much as a contact high from illicit practices.

But does greater consumer intelligence, Google terms enforcement and RankBrain mean that SEO is ready for eternal rest?

The real truth
Your prospective clients are smarter. They search conversationally with Google Now and Siri. They look at ratings, their friend's endorsements and "social proof."

Google is smarter. They hold websites to higher standards. They are also thinking about search result delivery in terms of topics rather than keyphrases. But change doesn't equal death — it just requires a strategy that evolves with the environment.

SEO offers incredible ROI
Even with all of the obstacles that come between your website and consistently ranking high in search results, SEO delivers more leads for less. When comparing fully funded PPC (pay-per-click) campaigns against SEO campaigns, we see the true value of natural traffic (for this experiment we used the highly competitive personal injury market).

PPC Only
Average cost per conversion: **$845**

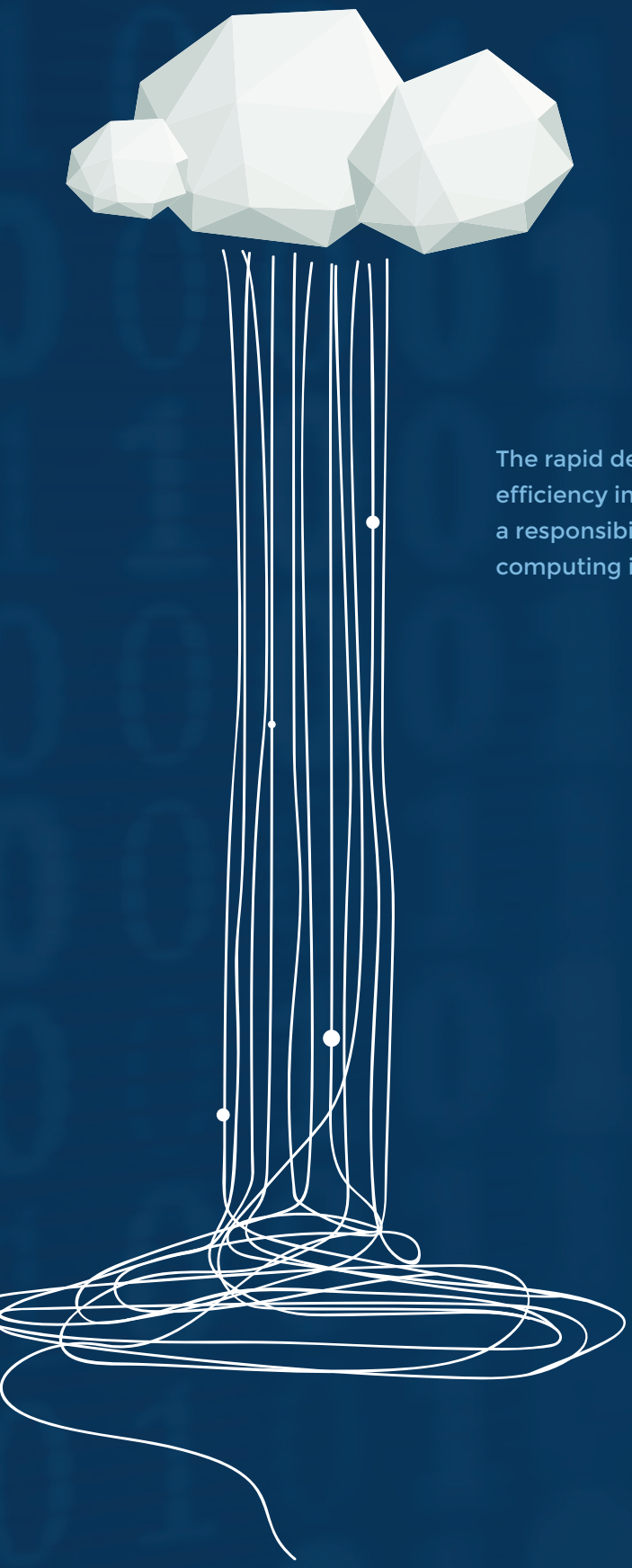
SEO Only
Average cost per conversion: **$220**

Of the SEO campaigns reviewed, the average website had 25 percent or less keyphrase visibility with an average monitored list of 3,000 keywords.

Consumers are smarter. Search engines are smarter. And yes, SEO is more strategic and will cost more as the process becomes more complex. But compared to paid advertising, SEO delivers the best value.

SEO isn't dead. It's just growing up.

- Jason Bland



security in the cloud

The rapid development of information technology has increased efficiency in law firms, and has also raised security issues. Attorneys have a responsibility to keep clients' confidential information secure, and cloud computing is of particular concern in this regard.

In the context of law firms, the term "cloud computing" most often refers to law practice management software or another type of software that is not hosted on the firm's own computers, but is accessed over the internet through a web browser. Such programs are also called "software as a service," or SaaS.

More broadly, cloud computing may include any situation where data that belongs to the firm or the firm's clients is physically stored on off-site servers. Under this definition, any third party data backup service may be thought of as cloud computing.

Regardless of the terms used to describe it, any situation where client information is stored outside of the firm's direct control raises the same types of security concerns. Attorneys and law firms generally recognize the duty to adhere to security standards, but a problem may arise in identifying just what standards are to be followed.

State Bar and ABA Standards

Attorneys are bound by the rules of their state bar association. According to the American Bar Association, only 20 states have issued ethics opinions that specifically address cloud computing. Attorneys outside of those states must refer to their state's more general rules regarding the security of client information.

As for the states that have addressed cloud computing, the ethics opinions vary in their details, but the ABA reports that they all permit cloud computing to be used, and all impose the standard of reasonable care on attorneys using such technology.

Rules and guidance vary widely from state to state. New York State's ethics opinion states that attorneys should investigate the security practices of a cloud computing vendor, ensure that the vendor has an enforceable obligation to preserve the confidentiality of information, and use available technology to protect against foreseeable attempts to infiltrate information systems. California's opinion states that attorneys should consult an expert if their own technological expertise is lacking. Connecticut's rules require that an attorney's ownership and access to the data not be hindered, and that the data be segregated to prevent unauthorized access, including by the cloud service provider itself. Florida attorneys should ensure that a provider will give notice if served with process.

The ABA itself has also addressed the ethics of cloud computing, by updating the Model Rules of Professional Conduct, to state that when dealing with information relating to the representation of a client, attorneys should make reasonable efforts to prevent unauthorized access or inadvertent disclosure of such information. The Model Rules state that attorneys should weigh the costs and benefits of additional safeguards to protect client information.

Legal Cloud Computing Association Standards

With the majority of states so far declining to issue guidelines that specifically address cloud computing, the Legal Cloud Computing Association has issued its own set of 21 standards, which it calls "Version 1.0" of the LCCA Security Standards, to emphasize that standards that apply to rapidly-changing technology must themselves evolve.

It is important to be aware that LCCA is a trade association made up of cloud computing providers; state bar associations and law firms may wish to impose different standards than these companies suggest for themselves. Nevertheless, the LCCA's standards set sensible benchmarks, which are more detailed than many state bar ethics opinions that have so far been issued.

The LCCA standards are directed toward the providers of Software as a Service, and they focus primarily on disclosures and notifications that should be made to users. The standards state that providers should have clear Terms of Service that define the provider's obligations and how performance is measured, and a clear and enforceable Privacy Policy that discloses how the user's data is stored, shared, manipulated and disposed of.

MOST STATES HAVE NOT ISSUED ETHICS OPINIONS ON CLOUD COMPUTING SECURITY.

However, firms that do use third-party cloud computing services still need to follow standards to ensure client information is safeguarded.

Providers should explicitly state that the user owns their data and the provider cannot acquire any rights to it, and they should notify users in the event of a data breach or a third party demand for data, unless prohibited by law from doing so. According to the standards, providers should also maintain encryption protocols covering data in storage and in transit, and disclose how frequently security protocols are tested. The full list of standards is available at legalcloudcomputingassociation.org.

The future of cloud security

Most states have not issued ethics opinions on cloud computing security, while those that have instruct attorneys to use reasonable care in ensuring that clients' confidential information is protected. Most lawyers are not information security experts, and firms will therefore rely on in-house or outside experts to advise them on technical matters such as encryption protocols employed or levels of certification obtained. The LCCA standards are an excellent starting point for firms evaluating the security of a cloud computing service. However, there are more general concerns that law firms should be aware of as cloud computing technology develops.

One important issue is government access to data by circumventing encryption, either through a proposed built-in encryption "backdoor" or by demanding that a cloud computing provider break existing encryption. Law firms whose clients may be vulnerable to such risks should take necessary precautions to ensure that the firm itself is the ultimate gatekeeper of clients' confidential information.

A related concern is the access that cloud computing providers themselves have to law firms' data. While all reputable providers encrypt user data both in transit and in storage, the provider itself is usually able to access the information, and the only protection that firms have from unauthorized access or use of the data by the provider is its obligations under the service contract. However, technological solutions to this problem may soon be developed. SpiderOak, a cloud storage provider, pioneered a "zero knowledge" encryption system which prevents the provider itself from having any access to the user's data. The company is currently developing a "team feed" style workplace collaboration software that will also follow the zero knowledge protocol. As such techniques continue to be developed, law firms may demand such a protocol for law practice management software in the cloud as well.

- Brendan Conley

enterprise social networks

[CAN THEY WORK FOR LAW FIRMS?]

ENTERPRISE SOCIAL NETWORK PROVIDERS PROMISE LESS HASSLE AND MORE COLLABORATION BY LETTING TEAM MEMBERS CONNECT INSTANTLY.

01 JIVE
Offers an interactive intranet and customer & partner communities.
www.jivesoftware.com

02 SOCIALCAST
Open communication between executives and employees.
www.socialcast.com

03 CONNECTIONS
A business social network powered by IBM.
www.socialcast.com

04 ASANA
Project tracking and team communication.
asana.com

05 YAMMER
Private collaboration across departments, locations and apps.
www.yammer.com

An internal communication system is another term for an enterprise social network. These networks provide a way for partners, associates, paralegals and other staff to interact from inside a firm's firewall. They are similar to chat suites or chat rooms, but in many ways different. Enterprise social networks are intended to foster staff cohesiveness, sharing, productivity and sensemaking within the firm's local network.

Enterprise network providers promise less hassle and more collaboration by providing an environment in which team members can connect instantaneously. Most enterprise platforms share several features, like private chat, the ability to create groups and teams and to communicate within those groups, calendering, notes, document uploads and task management. A law firm, for example, might create a group related to a particular case or client, or one specific to a practice group. Within these groups, people who need to collaborate on relevant issues could talk securely and privately, without interrupting the workflow of others at the firm.

As a business tool, enterprise social networks have been catching on quickly over the past several years, to mixed reviews. Businesses that have given an internal communication system a try voice numerous opinions about their effectiveness — both good and bad. Are these networks useful for law firms, or are they heading to extinction before they even get started?

One concern early adopters have voiced is whether such a system may actually foster isolation and detrimentally affect face-to-face interactions. Certainly this is a major issue in today's fast-paced digital world where sending a text or an email is quicker than finding and talking to a person in the same office. Is office camaraderie affected by internal communication systems? If so, how does a loss of human connection between staff affect productivity?

Another concern is the ability of instant messaging to interrupt much needed focus. How does being in constant communication with colleagues

affect an attorney's ability to get client work done? Do these systems work for all employees — everyone from senior partners and managers to mailroom staff — or only a few?

Enterprise social networks can work well in some business settings. Law firms have been slow to adopt these technologies, which is understandable given their ability to disrupt an already established workflow. These systems may not be ideal for every law firm where personal communication can be formal by necessity and collaboration is mainly done in person.

Restricted access systems

Restricted access systems exist within a law firm's firewall and are solely for the use of staff. The goal of these systems is to foster more open communication on all levels. Some of the more popular networks include Jive, Yammer and Socialcast, and the team communication platform Slack. As they have grown in popularity, a wide array of options have become available. Additional examples include Asana, Jostle Me, Tibbr, Convo, Kaltura, Chatter, Zyncro, Socialtext and Connections.

Despite the vast array of choices for firms interested in this kind of an internal communication system, it appears that less than half of such tools have many workers using them on a regular basis.

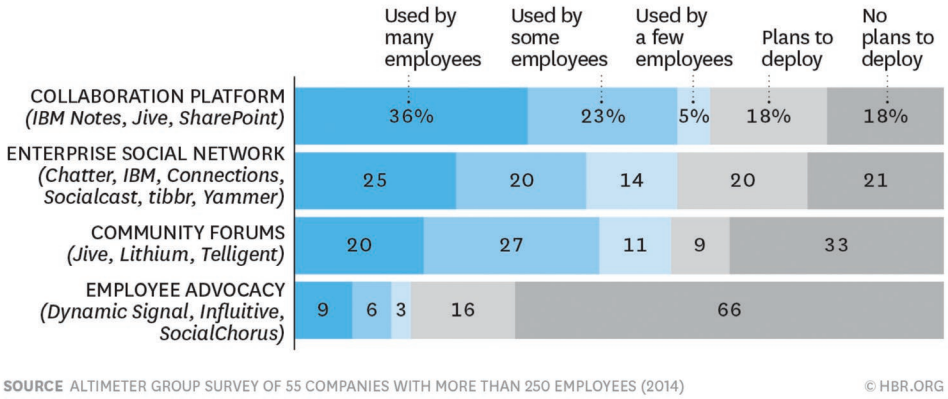
Why do internal communication systems fail?

It appears that many enterprise social systems fail because top executives and management do not view the engagement and collaboration offered by these internal communication systems to be a good use of their time. Furthermore, the perception appears to be that socially engaging on a chat-like internal communication system narrows the power distance between top management and their employees, diminishing their ability to command and control and be respected as capable managers. Top management rarely aspire to be "social friends" with employees.

In the C-suite world of law firms and other businesses, if something is not used, approved or supported — meaning the owners engage with it regularly and promote its use — chances are that staff will not use such systems either. Many managers and top executives view internal chat system to be detrimental to getting work done. Unfortunately, such an attitude misses the reality that such systems have the capacity to be bellwethers when it comes to identifying client, customer or staff problems.

However, the point now is that enterprise social systems have not yet reached their potential. They may be used incorrectly as more of a social tool than a problem solving tool, creating a place where staff play rather than work on projects. Until they do prove their worth on a wider scale, law firms and other companies

According to research by technology research and strategy company Altimeter, only 25 percent of enterprise social networks installed have many employees using them regularly.



may not consider using them. For an enterprise social system to work, a firm's leadership needs to be engaged in digital communication with all firm members and employees and have an open attitude about this communication.

Enterprise social systems as problem solvers

Consider the case of franchise giant Red Robin, with over 450 restaurants across the nation. To stay in touch, the senior vice president introduced Yammer. On the introduction of a menu item referred to as the "Pig Out Burger," employees used Yammer to alert head office that customers did not like the burger. Ultimately, managers discussed ways to adjust their latest offering on Yammer, and the product was revamped within a month.

Such an occurrence could have taken over a year to accomplish, and with much loss of revenue. This is an example of effective management and staff collaboration to solve a problem. Perhaps an enterprise social network in a large law firm may find uses for such a system that mimic Red Robin's. For example, if a large national law firm starts receiving communications from an office experiencing a significant increase in product liability cases relating to a certain drug, that office can notify other locations of the potential for cases to present themselves in other jurisdictions. This kind of communication, followed by action, allows more productive engagement and collaboration as well as a chance for employees to be heard by higher management.

Also consider the enterprise social network case study that involved UPS's implementation of Twitter in California. The company president chose Twitter because employees were already familiar with it. However, it was re-purposed into an internal communication system that sent out pertinent information to workers such as accident sites and route changes. UPS also uses Twitter as a company-wide employee recognition platform.

If management and owners can explore ways to use these systems productively within their firm's culture, their full potential may be explored. Traditional managers need to investigate how to move into the digital age of staying in touch at the speed of light in order to handle any problems that arise efficiently and effectively. Any enterprise social system tool can assist this process, but it is the thought leaders and invested partners who need to use the tools with purpose and intent in order to make the tool an effective one.

Enterprise social system issues

As with many other digital solutions that aim to improve communications between people and groups, there are glitches, gaffes, fails and bugs. The first generation of enterprise social platforms are stumbling toward a second generation (Enterprise 2.0), which may still carry some of the glitches of the first.

What is known about the failure rate of first generation enterprise social networks is that many are built with preconceived notions that do not fit a business milieu. For instance, the companies making these products assume everyone using one will jump on and collaborate, but the platforms are designed mainly to promote engagement between employees, not necessarily to be problem-solving workhorses. The enterprise social system also does not necessarily adapt well in the presence of a structured team order or established, existing law firm culture. It tends to be disruptive to existing work processes, can flood workers with information overload, and harbors the potential to have leadership decisions challenged digitally.

Ultimately, if your law firm has good communication offline, then an enterprise social network may work for you. As enterprise social networks become smarter, introducing a restricted access communication system to a firm may become more attractive. In the meantime, research and experimentation always lays the foundation for the incoming enhancements of the digital world.

- Kerrie Spencer

MORE LEADS

NO COMPETITION™

GET AN EXCLUSIVE LAW FIRM MARKETING PARTNER

Are you tired of your search engine optimization company helping your competitors rank higher than you ? You should be. Custom Legal Marketing is not a one-size-fits-all boxed solution. We commit to one law firm per practice area per city. We are only working for you.

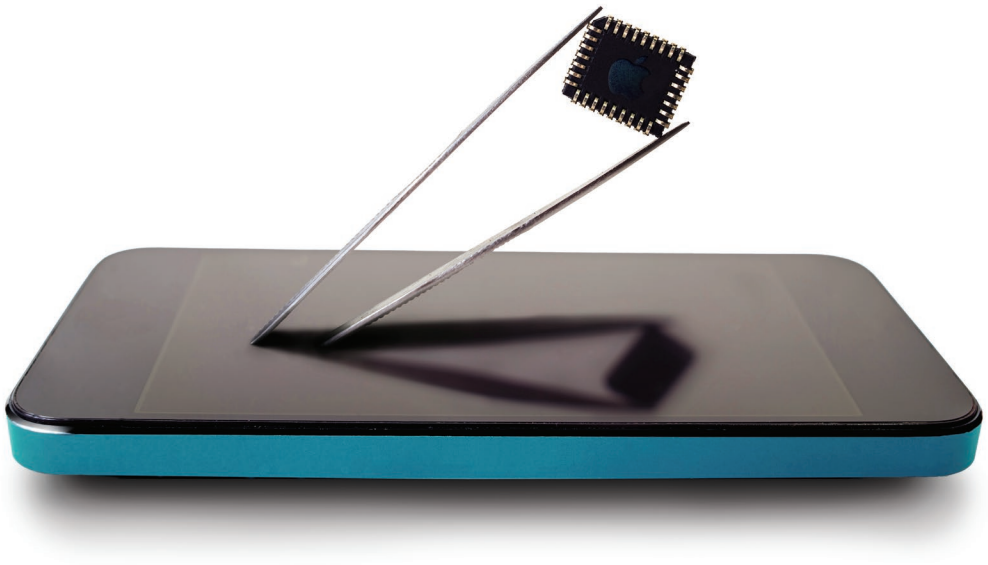
CUSTOM
LEGAL MARKETING

Inside

THE DIGITAL ARMS RACE: APPLE, THE FBI AND A LAW AGAINST SECRETS

On December 2, 2015, husband and wife Syed Rizwan Farook and Tashfeen Malik opened fire on Farook's co-workers at a training event and holiday party for the San Bernardino County Health Department. Fourteen were killed and 22 were seriously injured in what the White House called an act of terrorism.

After Farook and Malik were killed in a shootout with police later that day, the FBI searched the couple's Redlands, California home and discovered Farook's employer-issued iPhone 5C. Digital forensics analysts soon realized that the agency's best hope of unlocking the phone may have died along with the couple. A potentially pivotal source of evidence in one of the highest-profile crimes in recent history might prove utterly impenetrable to the nation's top investigators.



Apple, when presented with a warrant, has frequently assisted law enforcement in accessing certain data on older versions of its iPhone operating system. But newer versions, including the one running on Farook's device, cannot be compromised in that way. The FBI therefore sought a court order compelling Apple to create custom software bypassing some of the phone's fundamental security features, and Apple strongly objected.

Apple and the FBI geared up for a major new battle in the long-running fight over the balance between the security of encrypted communication and investigation of crimes. But on March 28, 2016, the FBI announced that it had successfully unlocked Farook's iPhone, circumventing its security with the help of a party outside the U.S. government. The FBI ended its effort to compel Apple's assistance, and the battle was called off.

The greater question of whether companies' and citizens' use of and access to strong cryptography will eventually be curtailed by the courts or by Congress still looms.

The Order

Like many modern smartphones, Farook's iPhone was protected by a four-digit PIN, or passcode, and its contents were encrypted. The number of possible passcodes, at 10,000, does not by itself represent an insurmountable obstacle. But an optional extra security feature on the phone automatically erases its encryption key if ten incorrect passcodes are entered, rendering the phone's contents permanently inaccessible. Investigators could not determine whether the feature was enabled, but could not run the risk of destroying their chances of unlocking the phone.

PRIOR TO SEPTEMBER 2014, APPLE WAS ABLE TO EXTRACT CERTAIN DATA EVEN FROM LOCKED, ENCRYPTED IPHONES, WITHOUT INSTALLING CUSTOM SOFTWARE AND WITHOUT KNOWING THE PASSCODE. THAT'S BECAUSE SOME OF THE DATA REMAINED UNENCRYPTED.

On February 16, 2016, U.S. Magistrate Judge Sheri Pym ordered Apple to help the FBI unlock and decrypt the iPhone. The assistance would come in the form of the creation of new software for the phone, which would disable the auto-erase function, allowing the FBI to "brute force" the passcode. In other words, they would simply enter every possible PIN in succession until they happened upon the right one — a task they could accomplish in minutes with the aid of computers.

The FBI probably could, in fact, create its own custom software that would allow a brute-force attack on the iPhone's passcode. What it can't do is install and run that software on any iPhone. Like many other devices, iPhones will only accept software containing a secret digital signature known only to the manufacturer.

In its filing requesting the order, the government invoked the All Writs Act of 1789, a catchall statute that allows courts to issue orders compelling individuals or companies to perform some action. Apple says this application of the Act is "unprecedented" in that it would force them to remove vital features of their product. The company says no other government has asked it to do what was being requested in this case — not even Russia or China.

Apple closes a loophole

Apple increased security significantly with the introduction of iOS 8, which included upgrades that kept all of the user's sensitive data under the encryption umbrella. The phone must be unlocked with the correct passcode in order to access any user data.

Apple was not shy in pointing out the implications of beefing up the encryption. With the introduction of iOS 8, the company said on its website, "it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession." That's why the government argued they must turn to this new strategy of compelling Apple, via the All Writs Act, to create custom software that enables brute force discovery of passcodes.

False hopes, false fears

It seems unlikely for two reasons that Farook's iPhone contains any data valuable to the investigation. First, Farook and Malik went to the trouble of destroying two other phones beyond the point where forensic analysts can recover any data from them. They also removed their home computer's hard drive, which investigators have been unable to find. They left the iPhone in question at their home during the attack, so it presumably played no logistical role in the attack itself.

Second, the phone was issued to Farook by his employer, which retained ownership of the device as well as control over the phone's account on iCloud, an Apple data-backup service. The phone's contents were not backed up to iCloud for a period of six weeks leading up to the attack — a lapse that could indicate either an attempt by Farook to hide information, or an ordinary lack of data diligence. Nevertheless, the employer's control over iCloud accounts for company devices was common knowledge among employees. For Farook to elect to conduct incriminating activities on this phone instead of his personally owned and controlled devices, which he took pains to destroy, is difficult to imagine.

If the FBI's professed hopes for finding valuable clues on the iPhone are dubious, Apple's argument in resisting Judge Pym's order is perhaps even more so. In an open letter to Apple's customers, CEO Tim Cook claimed that the software circumventing the iPhone's security features "would have the potential to unlock any iPhone in someone's physical possession." But the order explicitly required the newly-created software to be uniquely tied to Farook's iPhone. This would be accomplished by incorporating references to unique identifying codes present in certain components, such as the cellular and Wi-Fi radios. If someone then tried to install the software on another iPhone with different components, the process should fail.

Furthermore, the FBI was not seeking to have Apple hand over the software they create. The court order allows for the iPhone to remain in Apple's possession

while they install the custom software, with the FBI having remote access to the device. Under those circumstances, it seems, at first glance, very unlikely that the software could end up in the wrong hands, as Cook claims he fears.

In the court of public opinion, both the FBI and Apple are appealing to fear rather than reason. The government wants the public to believe that terrorists can only be stopped with assistance in bypassing or hobbling smartphone security features. And Apple would have us believe that the custom software they may end up creating would amount to a backdoor into anyone's data at any time.

It's the precedent that matters

Superficially, neither party's argument is compelling. Nevertheless, the aborted legal battle would have had huge consequences in the precedent it set. Cyrus Vance, Jr., a district attorney in New York City, is on a mission to bring attention to the roadblock that phone encryption represents to law enforcement. He says his office's evidence lockers contain more than 150 iPhones running iOS 8 or 9, which they are unable to access. If the FBI had followed through and prevailed against Apple in court, state and local prosecutors around the country would no doubt have filed a flurry of motions requesting custom software from Apple under that legal precedent.

The extent to which the hack on Farook's iPhone can be applied to other devices remains to be seen, and the public, and even Apple, may remain in the dark on that matter. But it's safe to say this outcome represents a lesser victory for law enforcement than would a precedent for compelling Apple to do the heavy lifting.

In his letter to customers, Tim Cook said an FBI legal victory would create a slippery slope of increasingly underhanded surveillance of its customers. If the company must compromise its own security features, Cook says, later orders could force them to "build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge."

Are Apple's fears warranted?

While Apple may be overselling the immediate danger of creating custom software for the FBI, more subtle legal issues may in fact justify such concerns. In a February 18 blog post, Jonathan Zdziarski, an expert on iOS forensics, draws a stark contrast between services that Apple has rendered to law enforcement in the past — i.e., a simple copy of certain unencrypted data — and the software it is being asked to create for the FBI. The former, Zdziarski says, is a lab service, the exact methods of which are not subject to great scrutiny because they constitute trade secrets. The latter, on the other hand, is a forensics tool — an instrument. As such, it is subject to far stricter evidentiary standards.

An instrument used by law enforcement to carry out a method of investigation must be rigorously proven to produce replicable results. It must be validated by a third party such as NIST, the National Institute of Standards and Technology. It also must be made available to defense attorneys who want independent third parties to verify its accuracy. Zdziarski points out that these are all potential points of failure where the software could end up in the hands of criminal hackers or oppressive governments who might be able to use it for their own illegal purposes in spite of Apple's safeguards.

These concerns may have lain dormant in the Farook case, as both the suspects were already dead; there is no defense attorney to object to the reliability of any evidence discovered on the iPhone. But if a government agency successfully prosecutes the custom-software strategy in some future case against Apple, and other prosecutors seize upon that precedent, it's easy to imagine a worrying number

?

HOW CAN YOU PROTECT YOURSELF FROM BRUTE FORCE ATTACKS?

A startlingly simple way for encryption users to remove any question of brute force attacks against their devices is to use a secure alphanumeric password — one consisting of 12 or more random characters including letters and numbers. While each additional digit of a numeric PIN code increases the number of possibilities by 10, alphanumeric passwords that include both upper and lowercase letters multiply far faster. If special characters or even foreign language characters are included, the numbers become truly astronomical in short order. No government agency has publicly acknowledged having the ability to crack such a password by brute force. This option is available right now for attorneys, criminal suspects and ordinary citizens for whom the ultimate in security is worth a few extra keystrokes.

of people gaining intimate knowledge of the software's inner workings. Apple's fears of opening Pandora's box may be well founded after all.

A dystopian future?

On March 21, just one day before a scheduled hearing on whether Apple would have to assist the FBI, the agency asked to delay the proceedings. A third party had demonstrated a technique that might allow them to break into Farook's iPhone. One week later, the agency dropped its case, claiming the method was successful.

However, the broader dilemma remains unresolved. No third-party method for breaking into a given device can be assumed to work with other devices and operating systems, both present and future. And Apple seems committed to creating products impenetrable not only to governments, but also to the company itself, having already eliminated the technical loophole by which certain data remained unencrypted. If Apple is ever compelled to devise a way to bypass its best security features, it could then go to work making its security even better, fortifying its devices and software against exactly the vulnerabilities that allow such exploits.

The prospect of a perpetual cryptographic arms race between law enforcement and high tech companies can make an intervention by Congress seem attractive by comparison. Many legislators and top law enforcement officials have advocated for years for a legislative solution mandating a "backdoor" into all cryptographic devices and software. The backdoor would ostensibly be accessible only to the U.S. government, and only with a warrant, but civil liberties advocates have doubts as to whether those goals of secrecy and legal diligence could be met.

Even if companies could create backdoors accessible only to the U.S. government and only in cases of serious crimes, experts allege creating it would in fact be a fool's errand, transforming the government's digital arms race against tech companies into a war against the entire tech industry, its own citizens and the very concept of secrecy.

IF APPLE IS EVER COMPELLED TO DEVISE A WAY TO BYPASS ITS BEST SECURITY FEATURES, IT COULD THEN GO TO WORK MAKING ITS SECURITY EVEN BETTER, RAISING THE PROSPECT OF A PERPETUAL CRYPTOGRAPHIC ARMS RACE BETWEEN LAW ENFORCEMENT AND HIGH TECH COMPANIES.

Suppose Congress required a backdoor to be built into every device and application made in the United States. Many smartphone applications are created in foreign countries.

Would the government compel Apple, Google and others to exclude foreign encryption software from their app stores? What about applications loaded from unofficial app repositories? Would companies be required to monitor every user's smartphone for evidence of illegal cryptographic apps obtained through such repositories?

And if, at great expense and effort, even those apps were somehow kept off Americans' phones, determined customers would turn to web-based cryptographic software already available. Following this hypothetical scenario to its logical end, it becomes clear that if the U.S. Congress wishes to keep all non-sanctioned cryptographic software out of the hands of everyone in its purview, the government must monitor and censor all domestic internet traffic — we must become China.

Politically, such an outcome is utterly infeasible. But that does not doom us to a world where electronic evidence can never be uncovered. Numerous uncontroversial avenues for evidence collection remain available for law enforcement. Phone calls, emails and texts tend not to be encrypted, and user data and even encryption keys themselves are often backed up to vendor-controlled servers by default. In cases where police apprehend suspects, biometric login data such as facial or fingerprint scans are easily obtained, and suspects may even be compelled to give up passwords or PINs without violating the Fifth Amendment in some cases. Suspects savvy enough to avoid every weak link in digital security will remain a thorn in the government's side, but those are exactly the sort of people for whom a government crackdown on encryption software would be a non-issue.

Some are so fearful of a world where digital secrets remain secret that they would steer us down a dark road toward a point where surveillance is so pervasive as to eliminate any semblance of privacy. But long before we get to that point, we will realize that the road is far too dangerous, and we have far too much to lose by continuing along it. With privacy advocates, the tech industry and principled lawmakers leading the way, people will make the courageous choice to forge a new and better path.

- Ryan Conley

The risks of using social media:

COULD YOU BE HURTING YOUR BRAND?

In just half a year, the number of businesses using Facebook Pages rose from 40 million in April 2015 to 50 million in December 2015. Today, that number continues to climb. More than 72 percent of internet users regularly access social networking sites, and in the United States, people spend an average of 16 minutes per hour using social media. By 2017, the global social network audience is expected to reach 2.55 billion.

Such a widespread attraction of social media for individuals as well as firms has the potential to both enhance and disrupt the ways people interact and firms grow. While social media can provide spaces for lawyers to participate in conversations with peers and industry leaders, as well as generate leads through engaging with prospects and clients, it can also present significant risks if the platforms are not used carefully.

The biggest issue that arises from the increased popularity of social media usage for law firms is that traditional risk management policies and procedures were not made with social media in mind, and do not necessarily address issues that arise with the ever-expanding advances of social media sites.

For example, Facebook recently implemented a new feature for Pages in which businesses can more easily communicate with customers and clients using an instant messaging feature. The page now displays how quickly the business replies to messages: either within minutes, hours or days. While some firms may easily reap the benefits of this type of interaction and openness of information, some may use the feature in a way that will actually be detrimental to their brand. The feature makes the firm accountable for online customer service, and if it is not prepared to fully engage with the feature, then users may question the firm's commitment to its clients.

With so many rapid updates and advances in social network features, how can firms' risk management procedures keep up, and how can risks be mitigated?

Social media risks

Traditional risk management policies were not built to address the minute-to-minute use of social media by customers and employees, resulting in an increased difficulty for businesses to identify and prevent brand, strategy, legal and market risks. Other risks connected with social media usage are negative exposure that can cause a decline in trust and a loss of revenue, as well as reputational risk. In the event such risks are not eliminated or diminished, they can cause severe ramifications, such as fraud, loss of intellectual property, loss of privacy and lack of compliance with laws and regulations.

Use of social media can be a profitable source of marketing and an effective client outreach strategy for attorneys. But it can also be dangerous when an online comment goes against the ABA's Rules of Professional Conduct.

> A LARGE PART OF RISK MANAGEMENT IS RELIANT ON PEOPLE. EMPLOYEES OF A LAW FIRM MUST KNOW THE RISKS ASSOCIATED WITH HAVING AN ONLINE PRESENCE, AND UNDERSTAND THAT THEY HAVE A PART TO PLAY IN LESSENING THEM.

Both inexperienced and veteran lawyers can find themselves in unfavorable circumstances for inappropriate postings on social media. Recently, the ABA Journal reported that a Minnesota Senior Judge was publicly reprimanded for posting comments on Facebook about trials he was overseeing. The *Chicago Tribune* also reported a story involving an experienced attorney who posted pictures of exhibits in a federal court case on his Twitter account, accompanied by his analysis of the evidence. Although he removed them from his Twitter, the attorney still faces possible sanctions.

Although these cases may seem extreme, social media has opened the door to many other possible situations that can hurt a lawyer or their firm. In order to reap the benefits associated with social media usage, companies must find ways to recognize, monitor and manage its risks before any harm is committed.

Solutions: Social media risk management

Social media governance involves the creation of novel ways of handling the risks associated with social media. A management consulting services company called Accenture emphasizes the need for using responses, policies, procedures and technologies to address traditional risk management. Social media governance can include well-defined roles and accountabilities in a company and within areas that have been exposed to such risk. It can also refer to cooperation among business units, policies that concern the use of social media, risk tolerance levels, escalation pathways and a model for handling crises as they arise.

Processes involve the modification of operations in order to proactively evaluate and monitor social media risk. They consist of identifying social media risk for reputation, prevention of fraud, business interruption and intellectual property. Social media governance also pertains to the reduction or shifting of risk in a way that is practical and efficient. In order to perpetually monitor risks, communication with those in senior management must occur often enough to effectively handle social media risk.

Part of the process of identifying risks is recognizing business opportunities. For instance, in light of the company's strengths and weaknesses in using social media, the law firm should consider the potential for discovering new services through the suggestions of clients online, as well as partnerships that come about through conversations on social media.

The human element in risk management

A large part of risk management is reliant on people; thus, human behavior must be effectively managed. Employees of a law firm must know the risks associated with having an online presence, and understand that they have a part to play in lessening them. Law firms should strive to produce a risk-aware culture in which employees learn to recognize the exposure of the firm to social media risk, and know what they should do to assist in mitigating those risks. Employees at every level of the firm should be made aware of the rules and regulations set by the firm, and be held responsible for their behavior.

Tools to monitor risks

There are currently technologies in place that can expand the monitoring of social media risk by humans. Companies can use web crawlers to locate references to a company, determine whether the reference is positive or negative, and provide a report. In this way, reputational risks can be identified and responded to faster.

Companies can also use technologies to monitor activity on social media by their employees. For instance, Actiance Inc. offers a platform that assists firms with the management of social media channels by controlling access to applications, observing social media content to safeguard the value of the brand as well as data security, and capturing online conversations to offer more complete information as to how interactions are occurring.

Additionally, data mining and analytics can put some order to the confusion caused by millions of posts and tweets to provide guidance to those who are concerned with business strategy and marketing.

Use social media governance to protect brand identity

Be strategic about your law firm's use of social media in order to reap its benefits without harming your brand. In defining your policy standards, your firm should make certain that its social media accounts are representative of your brand standards. Pay attention to the look and feel of the accounts, the usage of tone, voice and language.

First, decide who will be responsible for managing the company's social media channels. Having one person or a small team of individuals manage these channels will help keep behavior and voice consistent. Then, determine a strategy for using social media channels to accomplish business objectives. Next, develop a policy that addresses employee behavior online in abidance to the firm's brand identity. The policy should provide clear rules and boundaries concerning the actions of employees both online and outside the workplace.

How lawyers can benefit from social media policy

Lawyers can benefit greatly from having a social media policy in place to prevent them from making inappropriate comments about their cases, as well as disrupting the consistency of the brand's voice or identity. Although lawyers are encouraged to have a strong internet presence by actively participating on such social media accounts as Facebook, Twitter and LinkedIn, attorneys should act responsibly while engaging on social media on their professional as well as their private accounts to avoid violating any Rules of Professional Conduct. Some lawyers choose to implement rules of thumb to remind themselves what is appropriate for online posting, such as only posting something that they would not be ashamed of appearing in a news headline. They should also discourage clients from creating posts relevant to their cases that can be used as evidence by the opposing party.

It can only be beneficial for lawyers to implement a social media policy that protects them and their clients from the risks of taking too casual an approach to the use of social media. By engaging responsibly, lawyers will enjoy the advantages of an increased internet presence without harming their profession.

- Roxanne Minott

RISK + REWARD

An effective social media policy should aim to generate a competitive advantage while diminishing loss. In addition to establishing standards of employee behavior, it seeks to safeguard information that is confidential or proprietary, comply with legal rules, and explain the steps involved in managing crises in the event an error occurs.

Until recently, lawyer substance abuse was akin to the iceberg that sank the Titanic – only the tip of the problem was visible.

Inside the legal profession's DRINKING PROBLEM

A recent study reveals that one-third of lawyers have a dangerous relationship to alcohol, and lawyers are almost twice as likely to struggle with alcohol abuse as compared to the general adult population. The issue is far larger than most previously believed.

Approximately 10 percent of the general adult population suffers from alcohol dependency. Studies relating to alcoholism affecting lawyers have revealed the rate of alcoholism sits between 15 percent and 24 percent, which means that approximately one in five lawyers are addicted to alcohol. Further studies have also indicated that the stressful nature of the law profession, as well as that of the medical, dental health and social work niches, may cause many working in those fields to develop chemical dependencies, most often alcoholism.

The statistics prompted the authors of a study in the Journal of Addiction Medicine to conclude: "Attorneys experience problematic drinking that is hazardous, harmful or otherwise consistent with alcohol use disorders at a higher rate than other professional populations. Mental health distress is also significant."

So what is it about the legal profession that causes so many lawyers to become dependent on alcohol or chemical substances? Work-related stress and emotional alienation are common experiences for lawyers. But the problem can begin long before the individual begins their career. The problem originates for many in law school, according to Hon. Robert L. Childers, of the Circuit Court of Tennessee, who has served on the ABA Commission on Lawyer Assistance Programs (CoLAP) since 1999.

A closer look

A study revealed that 27.6 percent of the lawyers questioned had drinking issues before going to law school, 14.2 percent acquired the habit during law school, 43.7 percent developed the dependency within 15 years of graduating from law school and 14.6 percent began problem drinking more than 15 years out of law school.

Many who enter the legal profession do so knowing that they are pursuing an honorable career. They may choose to study law because they are driven by their moral values, are passionate about helping others or have a strong interest in the law. However, law school can challenge students not only intellectually, but also emotionally, and they often turn to alcohol or drugs to cope with mounting stress and unhappiness.

According to studies, law students report using alcohol to "get away from problems" and "relax and relieve tension." Such feelings often result from factors such as stress caused by excessive workloads and competition among students, as well as the tendency to rely on academic success to build a sense of self-worth. When students fail to live up to self-imposed standards, they are at risk of developing lower self-esteem. Students may be intimidated by teaching styles or other students, like overachievers or perfectionists. Some students may lose the connection with their original reason for wanting to attend law school, and may feel discontent with being trained to ignore emotional reactions in order to represent positions that are in opposition to their own moral beliefs.

Work-related stress is a common factor in the high incidence of alcoholism among lawyers. In their profession, lawyers help others solve problems, but they may find themselves struggling to ask for help themselves. Because of the sensitive nature of the legal profession, lawyers must often conceal their own emotions in order to deal with difficult cases and help their clients prevail. They may experience pressure to emote very little at the work place, which may hinder their ability to connect with co-workers. It is unsurprising, then, that many lawyers may experience alienation, which can lead them to look to alcohol to cope with their anxiety, stress or depression.

Additionally, social drinking, which is a common aspect of a law firm's work culture, can also encourage the issue.

Potential negative effects

Overuse of alcohol can lead to several potentially destructive consequences. The attorney in question may lose his or her job, be accused of legal malpractice or lose family and friends. Approximately 90 percent of serious disciplinary matters involve alcohol abuse and over 60 percent of all malpractice claims involve alcohol abuse.

Additionally, other important aspects of maintaining a successful practice may be adversely affected if a lawyer is suffering from substance abuse. Marketing is one of the most important areas for attorneys and law firms to prioritize during their practice to gain clients. If alcohol impairment affects a lawyer's ability to focus on marketing and business decisions, the attorney and his or her law firm face reduced productivity. An initial loss of productivity in business development activities will eventually result in lost revenue and eventually an inability to sustain a practice.

Lawyers experience significant levels of stress and anxiety, with 28 percent of attorneys suffering from depression, 19 percent experiencing anxiety and 23 percent reporting they were victims of high stress levels.

Is help available?

It is not just lawyers who tend to overuse alcohol. The whole legal profession, including judges and other officers of the court, are at risk. Recent findings beg the question:

What is being done to assist those in the legal profession with substance abuse issues now?

In 1988, the American Bar Association (ABA) launched its Commission on Impaired Attorneys, and in 1990 the Canadian Bar Association (CBA) asked a committee to study addiction in the ranks. Now, programs that provide support to those in the legal profession suffering from alcoholism, chemical dependencies and mental health issues are referred to as Lawyers Assistance Programs (LAP), and they exist in most states and all Canadian provinces. In fact, the problem is so prevalent that there are now three LAPs in New York alone, programs in 50 states and five in Canada, in addition to those in Wales, England and Scotland. It is truly a global issue. And today, the ABA mandates that a segment of CLE hours be devoted to the topic of substance abuse.

Although there are support and treatment groups designed to assist attorneys with substance abuse and mental health issues, many lawyers are hesitant to seek help because they fear breach of privacy in group sessions and do not want anyone to find out about their issues. This is why the LAP places a strong emphasis on confidentiality. Anyone seeking help from LAP should expect everything to be kept in complete confidence — it's the law. LAPs in most states respond to calls 24/7, and they offer free services to bar applicants, judges, law students and practicing attorneys.

Attorneys with substance abuse problems can have access to the help they need. However, they need to overcome the fear and hesitation to seek that help in order to continue with their careers and get their lives back on track.

- Kerrie Spencer

FOCUS
& The Myth of Multitasking

The ability to multitask may seem like a prerequisite for being a successful attorney. However, many studies have found it to be a counterproductive habit that reduces efficiency while increasing stress levels. Instead, experts say focusing on one task at a time is likely to yield better results.

A day in the life of an attorney tends to be filled with mounting piles of work and endless tasks to squeeze into an already packed schedule. In order to catch up, lawyers are compelled to work faster, put in longer hours or do more things at once. As a result they often juggle many tasks simultaneously, whether it is talking to a client on the phone while drafting an email, or catching up on paperwork while following court proceedings.

Lawyers may think they are accomplishing a lot by multitasking. However, multitasking simply creates an illusion of productivity. There is a growing body of research that shows doing too many things at once actually hurts both efficiency and quality of work rather than improving productivity.

The Multitasking Misnomer

Multitasking is the act of spreading one's attention over multiple activities simultaneously and trying to perform two or more tasks at the same time. For example, an attorney might check email while eating a quick lunch, marking the draft of a brief and listening to a muted conference call. While the practice is extremely common today, experts say in reality there is no such thing as multitasking. The habit can more accurately be described as "task switching," which involves rapidly jumping back and forth between different activities rather than doing them simultaneously.

Although human beings possess task-switching abilities, studies show they are not wired to effectively accomplish multiple activities at the same time when both require conscious thought and are controlled by the same part of the brain. It is possible to perform higher-level tasks simultaneously with automatic behaviors, such as walking and talking, or listening to music while eating. On the other hand, if an individual is chatting with a coworker while drafting an email, one activity will inevitably suffer. This is because writing and speech-related tasks compete for attention from the same location in the brain's prefrontal cortex.

Negative Side Effects of Multitasking

The common assumption is that multitasking creates efficiency. However, research shows people who multitask have significantly poorer time management abilities than those who do not. A 2009 Stanford University study found that constantly shifting from one area of focus to another makes heavy multitaskers worse at both filtering out irrelevant information and using their working memory — two key abilities attorneys require.

Psychologists claim the brain is not designed for heavy-duty multitasking. In fact, mental "juggling" can be harmful. Neuroscientist Dr. Daniel J. Levitin discovered in his research that constantly switching tasks depletes the brain's levels of glucose, which is required for effective thought and action. In response, the brain releases the stress hormone cortisol, which clouds thinking and leads to an endless cycle of higher stress levels and less productivity.

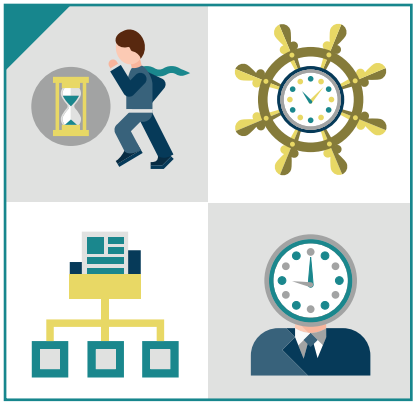
According to the American Psychological Association, performing more than one task at a time, especially multiple complex tasks, takes a toll on efficiency and results in more mistakes. The brain takes an average of 25 minutes per switch when transferring attention from one task to another. Moving back and forth between several activities means an individual wastes their attention on the act of switching gears rather than truly focusing on any single activity.

Attorneys can benefit from replacing multitasking with a new approach to time management. By slowing down and making an effort to stay focused on one task at a time, lawyers are likely to increase productivity, make fewer mistakes and boost mental wellbeing. Here are some ways in which attorneys can avoid the multitasking trap and deal with all the demands on their time and attention:

1 Remove Distractions

In today's screen-saturated world, people are constantly shifting between online and offline activities and dealing with an overload of information. Consequently, the art of single-tasking has become a challenging one to master. Attorneys find themselves juggling phones, laptops, iPads and other devices that demand their attention. With so many distractions at one's fingertips, the ability to focus on and finish a project before moving on to the next has become increasingly elusive.

Eliminating distractions can help prevent interruptions that can waste valuable time and make it more difficult to get back into the flow of productivity. According to Gloria Mark, informatics professor at the University of California, Irvine, the average person's attention switches every 45 seconds. Her research found that interruptions lead people to change not only their work rhythms but also strategies and mental states. She said, "Once thrown off track, it can take some 23 minutes for a worker to return to the original task." In addition, people compensate for interruptions by working faster, leading to more stress, frustration and effort.



Email is often a big culprit when it comes to multitasking. Many attorneys stop every few minutes throughout the day to check their email. Mark suggested limiting reading and replying to email to several 20-minute chunks of time throughout the day. Doing so can enhance efficiency by reducing the number of transitions between tasks and freeing up time for other work.

Additionally, blocking time in one's schedule to focus on high-priority tasks can also be beneficial. The aim is to work uninterrupted during this period instead of succumbing to distractions from phone calls, emails or drop-ins. If necessary, turn off email alerts and other notifications, or switch the phone to silent mode.

Learning the difference between true emergencies and tasks that can be scheduled for later requires practice and planning. Rather than attempting to do everything all at once, start asking whether the many tasks that come up throughout the day really require immediate action.

2 Recognize Not Everything Is Urgent

In his pioneering 2009 study, Stanford professor Clifford Nass challenged the notion that people could multitask with digital devices, such as talking on the phone, browsing the internet and checking email. Nass and his research team found that individuals who are regularly assailed with several streams of electronic information have trouble paying attention, controlling memory or switching from one task to another in comparison to those who concentrate on a single activity.

Attorneys tend to have many things vying for their attention simultaneously, several of which are likely to involve technology. For example, they may be juggling a ringing phone, a brief due the next day, an email notification, a client who wants to discuss their case right now and an associate seeking their opinion on a matter. It is important to realize not all of these situations are urgent. For example, the email, client and associate can wait until later.

Learning the difference between true emergencies and tasks that can be scheduled for later requires practice and planning. Rather than attempting to do everything all at once, start asking whether the many tasks that come up throughout the day really require immediate action. Decide which items are priorities and set specific times in which to complete them.

3 Practice Mindfulness

Mindfulness is the opposite of multitasking; it means paying close attention to what one is presently doing. Being mindful involves focusing on both the act of performing a task and the quality of the task. The practice can help reduce stress and provide a greater sense of accomplishment. Becoming more mindful can be as simple as shutting down an email program when starting to prepare a brief, or writing down a to-do list rather than feeling overwhelmed about remembering to do everything.

Although a direct correlation between multitasking and the outcome of legal matters may not exist, there are several implications. Besides a lawyer's productivity and wellbeing, multitasking can also have a negative impact on clients, who pay attorneys for their time and thinking ability. If a lawyer's brain is not completely focused on the client because of constantly switching between tasks, they may unconsciously be giving clients less than what they pay for.

Attorneys can benefit from a fresh approach in which they replace multitasking with focus-oriented work habits. While the lure of multitasking is powerful, understanding its hidden costs may help people choose strategies that boost their efficiency and daily job satisfaction.

- Dipal Parmar

MESSAGING: FOUR TIPS FOR CREATING GREAT BILLBOARDS

A billboard can introduce your firm to potential clients while building brand recognition within your local market. Not everyone who sees your billboard will be in immediate need of legal services; however, for certain practice areas especially, establishing a foundational awareness of your firm can be very beneficial. When the need does arise, people are more likely to choose a familiar name or face, rather than confront the uncertainty of hiring someone they have never heard of.

For all of their potential benefits, billboards can be tricky animals. Billboards are physically large. They provide a lot of space for design and messaging. With all that space available, the temptation inevitably arises to fill it up. But in order for a billboard design to be effective, it must be simple — sparse even. One or two bold colors, one short headline, and maybe one image — with an emphasis on maybe — are all you can afford to use on this medium.

Simplicity is a billboard's most important design element. The billboard's meaning, ideas and layout must all be easy to process. Poor readability or confusing wording will ruin a billboard. Too much text, the use of colors without enough contrast, unreadable fonts and distracting images can all cause your billboard to fade into the background noise.

Here are four ways you can avoid falling into advertising obscurity and produce billboards that work for your firm.

1. Choose your words wisely.
All good marketing copy should be simple and concise. And billboard copy has to be the simplest of all. Remember the number seven: seven seconds and seven words. After you have established an overall theme for your billboard, you will need to distill this theme to a point that you can express it in no more than six or seven words. Drivers cannot take in more than that in the seven seconds you have to get their attention.

Can motorists pick your billboard out from all the other advertising noise? They should be able to.

A good rule of thumb for judging the readablility of your billboard is the "business card at arms length" test. The proportions of a business card held at arms length are approximately the same as a billboard on a highway. So, put your design on a 3.5" x 2" sheet of paper, hold it up and look at it. If it is not clear to you, it will not be clear on the road.

2. Say it with color.
One of the best ways to add visual interest and impact to your billboard is with strong, contrasting colors. Paired with a bold, easily readable headline, color may be the only graphic element necessary. Color can demand attention, elicit emotion and convey meaning. The colors that you use to represent your firm's brand should be reflective of your corporate philosophy. Billboards can be a great place to let these colors work for you.

3. Pick an obvious focal point.
If you decide to use an image on your billboard, then you will have to work a little harder to avoid visual clutter. In order to keep your copy and your picture from competing with each other, choose one focus, and make it obvious. Do you want people to see the image first, then move to the copy as a support element, or the other way around? Whichever focus you choose, exaggerate it. Make it obvious, or you risk loosing the clarity of your message.

4. Break out of the mold.
If your budget allows it, go over the top — or maybe out the side. Billboards that break the rectangular shape are instantly more memorable. Chick-fil-a has mastered this strategy with their series of billboards involving their famous three-dimensional cows. In 2011, Coca-Cola created a billboard made of live trees that it claimed helped absorb air pollution. This practice doesn't have to be limited to elaborate designs and big brands. Law firms can take advantage of this trick, too.

SHOULD MY FIRM USE BILLBOARDS?

Billboards are not for every lawyer. If your firm offers specialized services that are not relevant to a wide range of people, then your advertising dollars will be better spend elsewhere. To take advantage of billboards, you should be able to easily make your pitch in one sentence or less.

- Kristen Friend

NOBODY LIKES TO BE LEFT IN THE DARK

While many law firm marketing companies put up walls between you and your statistics, we decided to install a window. Follow trends, view your link portfolio, track rankings, follow competitors and more in the newly redesigned CLM Lounge.

CUSTOM
LEGAL MARKETING