NYSBA FALL 2010 | Vol. 28 | No. 2

Inside

A publication of the Corporate Counsel Section
of the New York State Bar Association

Message from the Chair

On behalf of the Executive Committee, I am so happy to share with you some of the recent activities that the Section has been working on and ways in which you can get involved.

First of all, we are thrilled that the Kenneth R. Standard Diversity Internship Program is currently in full swing. It is one of the Section's signature programs and we have a full update in this issue of *Inside*. I would like to personally thank David Rothenberg, who is chairing the Internship Committee, and his team for all of their hard work to make this year's program a success. If you or your company would like to get involved with sponsoring students next summer or assisting in any way with the program, please reach out to him.

The Membership Committee has been working on various initiatives to increase the number of members in our Section, and also to provide services to our existing members. You will be receiving more information shortly about our upcoming Member Appreciation Reception which will tentatively be held on **Thursday, September 23**, in Midtown Manhattan. We are always open to ways in which we can better serve our members, and ideas are always welcome.

The CLE Committee is planning a series of informative educational events, including a Fall Ethics Program in November, a CLE in conjunction with the International Section on Updates to the Foreign Corrupt

Inside

Editors: Janice Handler and Allison B. Tomlinson

Special Issue: Law and Technology

Practices Act in the early Fall, and other interesting and practical topics. If you would like to propose future topics for CLEs, please reach out to Howard Shafer or Steve Nachimson.

The Technology Committee has been working closely with the Bar Association on updating our website, and implementing new and innovative ways to reach out to our members. Again, if you have any ideas or are interested in working with that Committee, please contact Fawn Horvath or Julie Ko.

The Inside Committee continues to strive to bring you timely and useful topics, with this issue focusing on Technology Issues and the upcoming edition being centered on Employment Law. If you would like to contribute an article to *Inside* or have ideas about future theme issues, please contact Janice Handler or me.

And for those interested in Pro Bono activities, we sent an announcement about volunteering opportunities through the Pro Bono Partnership by e-blast to the members. For more information, please go to www.probonopartnership.org.

We have also been working on bringing additional services to the members, and will be using e-blasts to send you this information over the coming months.

Thank you for your interest in the Section. We are here for you, so please feel free to call or email us at the contact information listed on the last page of *Inside*, with your ideas and thoughts.

All the best,

Allison B. Tomlinson

Inside Inside

The Death of Footnotes

This issue is another blockbuster special issue on Lawyers and Technology. No, not your own technology—though heaven knows, we could use some help with that! We focus on the legal issues created by the new technologies and the places where they intersect you and your company. Our authors are specialists in the e-age and from Mark Grossman's savvy real world overview to more specific pieces about social media, monitoring employees, e-discovery and FTC red flag rules, there is something here for you whether you are a technophobe or a CrackBerry baby.

You might note that some of these articles have no footnotes. While we have nothing against footnotes (Janice quite likes them in her day job as a law professor) the lack of them highlights our commitment to useful, practical, real world pieces designed to interest the corporate specialist and educate the corporate generalist. We know that most of you do not spend your days reading cases. You spend your time looking for hard-headed solutions for real world problems. *Inside* is committed to helping you do that—so let's drink to the death of footnotes.

Janice Handler
Allison B. Tomlinson

What Is "Tech Law" Anyway?

By Mark Grossman

If you're a seasoned General Counsel, they didn't teach you technology law in law school because it was a legal specialty that did not really exist before the late 1980's at best. Now your problem is that your company lives in a mostly paperless, online world and you are concerned (at least privately) that you are not particularly comfortable with the legal implications of computers, the Internet, e-commerce, privacy, employee rights online, cybercrime, technology use policies, contracted for IT-related goods and services, and a host of other interrelated issues. The purpose of this article is to give you a brief overview of a few of the technology law issues that you must have on your radar. The articles that follow will add some depth on some of these subjects.

Let's start with a fundamental question: "What is Tech Law anyway?"

To answer this question let me first give you a little bit of background. I started describing myself as a lawyer with a practice that focused on "computer and tech law" over 20 years ago. When I would tell people this 20 years ago, they look at me somewhat quizzically. You know—the same look you would expect if you had just told them that E.T. was in your yard.

After that "look" went away, they would typically ask me two questions. What exactly is a "computer lawyer" and can you make money doing it?

The answer to the first question is somewhat nebulous, but I'll attempt to answer it in the next section.

As for the second question, nobody ever asks me that anymore. A couple of decades ago, I would say, "Sure you can. Really! Don't look at me that way. You can!" At least I hoped that I could in the world as it existed before the commercial Internet and even before what would be referred to the "Information Superhighway." Remember, that was back in a world before every employee with a phone on his or her desk also had a computer.

What's in a Name?

A lot has changed in 20-plus years. In that time, I've watched tech law and the issues that should concern in-house lawyers go through many incarnations. Even the name of what you call my specialty has evolved.

The list is long and includes computer law, Internet law, e-commerce law, cyberlaw and tech law. The names reflect the evolution of what was hot in the area. Today, I use tech law because I think my specialty encompasses all kinds of technologies.

Two decades ago, a computer lawyer did things like contracting for custom software development, protecting software's intellectual property (with heavy emphasis on the copyright side and light on the patent side), and technology-related litigation. The specialty developed because people were spending big money on technology and the typical lawyer in 1990 viewed the computer as the $3,000 typewriter on his or her secretary's desk.

Back in the 1980's and 90's one of the results of most lawyers being technologically challenged was that they were completely unprepared to deal with the contracting and litigation that arose from tech deals. You cannot ask the right questions if you are clueless.

While any good litigator can handle the "network is dead" lawsuit, or any good transactional attorney can negotiate a simple computer hardware purchase, it takes a bit more finesse and knowledge to handle issues such as the "network is slow," "the software crashes too often," or "the system is not performing to our expectations." One of the problems with tech law is that you have to work these mushy issues all too often.

Tech law and the need for expertise in this area have exploded in the last 15 years. It reflects the way technology and particularly the Internet have entered our lives. It's a clichéd joke to ask, "How did we survive before email, iPhones, and CrackBerries?" My answer is that I don't remember how we survived. Thinking back that far causes me to reflect on carbon paper and feeling older.

Think about it. It really was not that long ago that TV commercials and billboards were not obliged to send you to www.OurWebsite.com. You don't have to think back too far to remember when the high-profile Super Bowl commercials were the exclusive province of Chevy, Bud, and Pepsi—not www.I-Never-Heard-of-You-Before-and-Will-Never-Hear-of-You-Again.com.

What Tech Law Has Become

Tech law today is still about the same things tech lawyers did two decades ago, but now it is so much more. New issues seem to arise every day that need answers, and inevitably, it takes a while for the law to evolve.

What's scary about this process is that the Internet and technology have wrought many fundamental changes to our society and companies and, in many cases, the people legislating are not particularly sophisticated about our online world. I have a problem with legislation impacting our interconnected world being influenced by a person who thinks that surfing the Web means watching his grandkids playing video games.

Still, a fundamental truth about technology and law is that first we develop new technologies and then we have to figure out how to regulate them. On that level, nothing has changed during my 20 years of practicing tech law and the process will never change. After all, someone had to invent the telephone before we could legislate on the abuses of telephone marketing. Likewise, we needed the ability to enter into agreements electronically before we needed the Federal legislation called "E-Sign" to legitimize electronic signatures.

It turns out that even defining tech law is not straightforward because it is by its nature an eclectic specialty. I do not assume that the term even means the same thing to practitioners who describe themselves as technology lawyers.

For example, the bulk of my practice revolves around business deals. So, when I describe myself as a technology lawyer, what I mean is that I am a deal guy who focuses on sophisticated deals involving anything that touches technology, telecommunications, and outsourcing (whether outsourcing IT or other things like business processing). The deal could be things like a complex managed services, SaaS (software as a service), software development or website hosting and development deal.

I think most other lawyers who describe themselves as tech lawyers are intellectual property (IP) lawyers who focus on the IP rights that flow from and around technology. Certainly, every tech lawyer must have IP law expertise because almost every tech deal has IP that needs to be sorted out clearly and unambiguously by the contract. Still, there's so much more to practicing tech law than just focusing on the IP aspects of the deal.

As a General Counsel, the hot button tech law areas for you will be an ever-evolving eclectic bundle of legal concerns.

Company Website

Let's start by looking at some of the tech law issues relating to your company's website. After all, it is the world's portal into your company.

Does your company own the copyright to its own website? If it was developed by an employee, the answer is probably "yes" because the law concerning ownership of copyrights created by employees is basically intuitive. If an employee created it as a part of his or her duties as an employee, the company probably owns the website.

Still, an agreement with an employee on IP is still a best practice because that agreement helps you avoid hearing things like: "I did it on my own time," "in my garage" (why this stuff happens in garages still baffles me), "outside of the scope of my duties," and while "using my own computer."

The law concerning independent contractors is counterintuitive in that the independent contractor will own the copyright for your company's website unless you have a proper written agreement to the contrary. This is one big trap for the unwary and the generalist General Counsel who is not familiar with IP law.

The website also raises privacy issues and concerns that come at your company from all directions these days. For example, Massachusetts has been the center of attention recently because of a comprehensive privacy law designed to protect the personally identifiable information of its residents.

Moreover, if you think that this new law does not impact you because your company is not located in Massachusetts, think again. We live in an interconnected world where state jurisdiction due to online contacts is a fact of life. Can you really be sure that you don't have a customer or employee (current or former) who is a Massachusetts resident?

One of the problems with the legislative and regulatory framework that governs our online world is that law comes from the Federal government and each of the 50 states. Oh, and let's not forget about every other country in the world. This patchwork of often conflicting laws and standards makes it quite difficult for the generalist lawyer to stay afloat.

Electronic Discovery

Next, let's look at tech law issues relating to electronic discovery. Litigation and electronic discovery are a huge nightmare for many in-house lawyers. That's not surprising since electronic discovery was barely a blip on anyone's radar not too long ago and now it is often the core of discovery in commercial litigation. The days of delivering boxes of paper are over. Now, you routinely see million-plus document cases where the parties are using sophisticated computer searches to find relevant material.

There is a steep slippery slope here when dealing with electronic discovery, where the line between routine business practices and spoliation of evidence is a narrow one. Here is yet another area where a lawyer who is comfortable with technology and can go toe-to-toe with IT professionals in discussions about database queries, backups, data formats, and other related issues is essential. It is not too hard to find your company being sanctioned by a court due to electronic discovery missteps.

By the way, if you wait for litigation to think about your IT procedures designed to preserve evidence in case of litigation, you are probably too late. You will be playing catch-up in a game with hefty sanctions staring at you.

Educating Your Employees

Finally, let's look inward to your employees. Every—and I mean **EVERY**—employee with Internet access needs training about the fundamentals of the law concerning the Internet. The ways your employees can cause legal issues for your company online are endless.

To some extent, the problem is that the Internet is still relatively new in the workplace and with that newness comes many misconceptions that could become your nightmare. I cannot even begin to count the number of sophisticated business folks who are just wrong about some of the fundamentals concerning the law online. It is simply naïve to think that your lower level employees understand this stuff when the sophisticated often do not get it.

I find that I am often introducing new concepts to people when I say things like "copyright law applies online" or "what you say online can constitute libel as if you said it in a magazine."

This segues nicely into one of the newer hot button things for General Counsels to lose sleep over—social networks. While it is true that the simple answer is to prohibit employees from using social networks at work, this is probably self-defeating.

Most companies want an online presence in places like Twitter, Facebook, and LinkedIn. While you can wistfully remember the days when controlling your company's message was easy because of the small number of folks authorized to speak on behalf of the company, the world has moved on you again.

Now, you probably want your employees online tweeting and interacting with the world online through social networking (and if you do not think you want this I think that I could make a good case that *you* are missing the boat). This type of messaging about your company is really not done well by just your PR folks. You probably need to let your employees loose in places like LinkedIn and Twitter.

My take is that the legal tail should not wag the dog. If social networking is good for the business, then the task for legal is to make the legal risks manageable—and you can do it. The path to this Promised Land is education and training, and clear company guidelines explaining the company's social networking policies. You cannot really expect your employees to understand the law online if you do not teach it to them and then give them clear guidance.

If there is any good news for the General Counsel who has to help his company comply with the law in an increasingly digital world, it is that you do not have to have a deep understanding of the technology to lawyer it. We are lawyers not techies. With a little knowledge of the tech stuff as background, you can then focus on the law and not the tech.

I would just encourage you to not offer conservative advice that hinders your business just because you do not feel comfortable in a digital world. I suggest that you and your company embrace all that technology brings to your bottom line. As lawyers, we must protect our clients from the new downside risks that technology offer, but do not be a naysayer. Find a way to make technology work for your company. Develop policies. Train employees. Provide legal guidance. And, most importantly, find ways to say "yes" when asked about introducing some new technology to your company.

Mark Grossman is a 26-year business lawyer who began focusing his practice on technology, telecom, and outsourcing deals about 20 years ago. Mark authored the book *Technology Law—What Every Business (and Business-Minded Person) Needs to Know*, and is a frequent speaker on technology law.

Website Reminder

The Corporate Counsel Section wants to feature its members in a new upcoming section "In the News" on our website. We want to hear about news, press releases, promotions, publications, events, pro bono, community involvement and anything else you think might be of interest to the community. So don't be shy, let's hear from you. You can send these items to:

Natalie Sulimani
Sulimani Law Firm PC
116 West 23rd Street, Suite 500
New York City, NY 10011
natalie@sulimanilawfirm.com

Tweeting and Liking Your Way to Brand Protection: The Practical (And Somewhat Tech Savvy) Guide to Protecting Your Brand Online

By Natalie Sulimani and John S. Morales

According to the definition by the American Marketing Association, the legal term for brand is a trademark.[1] While that may be true, and brand may not be possible without a trademark, a brand should be viewed as more than that. Saying that a brand is a trademark seems too passive, as if merely registering a mark, or marks, is enough to maintain one's brand. On the contrary, the owner of a brand has to be very active in building and policing that brand in order to build up goodwill in that brand and its marks, increase value in the market and avoid losing those marks and / or market share in the marketplace.[2] In this article, we will explore the steps brand owners need to take in order to build and protect their brand online with the advent of social media.

First, it is important to understand the difference between social media and social networking. There is a real distinction even though they are often used interchangeably. Social media is a way to share information with a wide audience through social networking. The brand owner can directly engage with people who have things in common. This is an outward act of communication. Social networking, on the other hand, is a two way communication between, in this case, a brand owner and the public. While it is harder to gauge the return on investment with social media, with social networking it is easier because it is possible to see the traffic on a site as well as how many more "likes" or "followers" from specific campaigns. There are other differences, but the main theme here is dissemination with social media versus engaging the public through social networking.[3] It is important in managing and promoting a brand online to keep these distinctions in mind while taking advantage and integrating both aspects into brand strategy.

Branding is becoming a critical part of marketing, especially in the online world. The very definition of a trademark is the association of a mark with the goods or services. The mark has to elicit specific images and information to consumers. Just like the distinctive red and white style on the can of Coca-Cola evokes in the mind the fizzy sweetness on the palette, consumers should associate the look, feel or even taste of a service or product when they see the mark. And it should be the look and feeling that the brandholder wants them to associate with the product. After all, an important aspect of trademarks, which has been recognized by the courts as well, is to cut down on consumer search costs, making it easier for the public to find the product.[4] The benefit to the mark owner is that more people will seek out the product that they know and will buy it more often than other products that have not built up the same goodwill in the consumer's mind. This goodwill in a mark means goodwill in the brand, so that the same red and white stripe associated with Coca-Cola will also be able to more effectively sell beach towels bearing this mark. That is the power of branding and the reason why it is important to pay close attention to how the marks are being used and discussed online.

The first step to brand protection is to own the intellectual property. While the laws of the Internet are slow to progress, protection of intellectual property is the best offensive to protecting the brand online. While one way to do that is to register the trademarks, such as name, logo or slogan, another great protection is copyright registration. Whether it is to register articles, blog posts, designs or even the website, copyright protection is part of protecting the brand offering and another line of attack against infringers.

Why is brand protection so important? It is easy to get lost in the massive amounts of information online, but at the same time, it can also be easy to differentiate from the rest through effective branding. Social media and social networking are especially suited to developing and maintaining the brand. Done the right way, connect to consumers, build a following and then remain relevant as the market changes. Doing so will help create customer loyalty and make it easier to sell existing and new products and services. At the same time, it can control any likelihood of confusion in the marketplace with other products, avoid dilution and more importantly genericide, and even control the cost of marketing. Branding online can also make it easier to quantify the return on investment. Social media allows one to monitor online campaigns. By using certain tools one can see what is and is not working in the online marketing strategy and make changes accordingly.

On the other hand, the effects of not monitoring the brand or letting someone else dictate how the brand is portrayed online can be devastating to the company. In such tight economic times, it is unnecessary to point out how every marketing dollar counts. The effects of brand abuse will bring a decline in revenue and more marketing dollars to offset the damage. It is important to remember that a brand can suffer from a death by a thousand cuts as easily as big scandal. For instance, if a competitor decided to use the mark in a pay-per-click campaign, without proper vigilance, it could easily divert consumers to its

products. To offset that kind of damage, one would have to pay more for one's own PPC campaign or more money for the web developer and search engine optimization (SEO). Moreover, allowing competitors or even consumers to use the mark generically, or in ways that are not unique to the brand, can risk the mark getting cancelled in the Trademark Office for becoming generic.[5] Next time you have a headache and turn to your trusty aspirin, take a moment and consider that aspirin was once a trademark.[6] The other effect of brand abuse can even be a harm to reputation and loss of goodwill. If someone should write a less than glowing review of the services on Yelp and you were not paying attention and did not respond in any way, the bottom line will reflect it. Mind you, the remedies are not always legal, but may have more to do with good old-fashioned business sense.[7] Well, that and a good web person. Given the terms and conditions of most of the review sites, a bad review is one thing, but when falling victim to a fake review by a competitor, sometimes the only thing to be done is bury it, bury it, and yes, bury it, *i.e.* make sure that the glowing reviews far outweigh the bad.

Here are some specific examples of brand abuse and what can be done about it:

Keyword or Pay-Per-Click Abuse. Websites cannot exist in a vacuum; you cannot get the message out there if there is no one listening. One measure of a website's success is the amount of traffic. Just like a brick and mortar store, there are several ways to drive consumers to the online store. There is direct traffic (they specifically typed in the URL), foot traffic (they were searching around the web for the product or service and found the site), advertising that directs people to the store (online ads with links to the website) and referrals (someone followed the link that was posted on another site). More than any other method, the Internet is uniquely situated to take advantage of cross promotion and linking. While direct traffic is nice, most of the time, people do a search, or "Google," and then find the website. Even there, there are two options, a "sponsored" ad or organic search. An organic search relies on really good search engine optimization (SEO). A good organic search depends on proper keywords, descriptions, tagging and things of that nature. Note, Google, as well as the other search engines, no longer pays attention to metatags so we can move on from there. Keywords, however, are a different story. They are, in a word, key. While most people will use their mark and a description of services as keywords, some people will use their competitor's mark as a keyword either with the SEO or by buying the keyword. Pay-per-click (PPC) advertisements are the sponsored ads you see at the right or top of the search page. Companies pay for keywords and Google has made it quite clear that it will sell registered trademarks as keywords. Other search engines have not engaged in this practice thus far. Google's argument is that there is no likelihood of confusion and that, technically, it is not a use in commerce. This attorney disagrees and so should any brand holder. As, in fact, the Second Circuit did, at least on the issue of "use in commerce."[8] Essentially, competitors are taking a free ride on the goodwill and marketing dollars to divert legitimate traffic from one site to theirs.[9] After all, didn't they search for your trademark? Keyword and PPC abuse is something you can monitor by having the proper analytics and alerts in place (analytics are a way to monitor who is visiting the site and how they are getting there). Some vendors are Google Analytics or StatCounter. Alerts are a way to monitor any mentions of the brand. A good source for this is Google alerts or paid monitoring companies.

Cybersquatting. While still a problem, it is no longer the cybersquatting of yesteryear. First, as a trademark holder, the remedies are laid out through domain name disputes administered through the Internet Corporation for Assigned Names and Numbers (ICANN). It is important to be the rightful owner of the trademark before pursuing a domain name action, meaning that the mark is federally registered or there is at least a common law claim to the mark. Gripe sites are still around, but for the most part, that's protected as nominative fair use under the Lanham Act or as free speech under the First Amendment.[10] The real threats now are the emails coming from abroad threatening to register sites overseas lest you pay them for those sites. Still, domain name disputes are cost effective and fairly straightforward under the Uniform Domain-Name Dispute Resolution policy. As long as the brand holder has a registered trademark and the cybersquatter has no legitimate use besides holding the site hostage, more often than not, the decision will be in the brand holder's favor, even if the defendant appears in court. Practically speaking, cybersquatters rarely show up to defend themselves—for every domain name lost, there is someone else down the road that would rather pay than litigate.

Defamation. This is a false statement that is harmful to someone's reputation, and published "with fault," meaning that one knew or should have known that it was false. Libel is a written defamation; slander is a spoken defamation. Defamation is determined differently by the laws of each state, but generally, the elements to prove defamation are:

1. A publication to one other than the person defamed;
2. A false statement of fact (this does not include opinions or statements of hyperbole); and
3. That it is understood as being of and concerning the plaintiff; and tending to harm the reputation of plaintiff.
4. If the plaintiff is a public figure, he or she must also prove actual malice.

One cannot sue under defamation for statements of truth. Another stumbling block with defamation is that although you may hold the party that wrote the defaming content online liable, you cannot reach the provider that posted the content because of the immunity provided by Section 230 of the Communications Decency Act.[11] Instead of defamation, you may find more success through trademark and copyright law in removing damaging information.[12]

False Association. This is a slippery slope on the Internet and subject to all the fair use defenses provided by the Lanham Act.[13] A brand owner must also consider the damage to the brand for being overly vigilant in this area. In a situation like *New Kids on the Block*,[14] even if the trademark owner were to prevail against the defendant, the result might be a lot of bad will against the mark and possibly irreparable harm to the brand through bad PR and "sucks" sites that are beyond the ability to control.[15]

Going back to the issue of SEO, linking is another way to increase website ranking, and here is where you need to rely on that good old-fashioned business acumen again. The question always is, "Do I want to be associated with this website?" It is a mistake to not allow other sites to link to your site and vice versa. After all, this is goodwill on the Internet. By utilizing other traffic sources to get your website seen, you can increase exposure exponentially. But that being said, you are giving them a license, and it is conditional. It is the nature of the Internet that sites are bought and sold. You need to be in control of who is linking to you and how. Should you decide that you do not like the association, you can revoke that license. This, again, is something that can be monitored with good analytics.

To Cease and Desist or Not. While you are monitoring a brand online, you should look for trademark or copyright infringement, defamation, cybersquatting, misappropriation of name, and general harm to reputation, to name a few. This is also where business sense is a must. While a cease and desist to the infringer is a good idea, weigh your options. Perhaps this is someone that can help the brand instead of hurting. If they are, consider a license that can be mutually beneficial. If you decide that the use is harmful, send a cease and desist. The first touch should always be the gentlest. You cannot assume that they are maliciously infringing, they might, in truth, have no idea that you exist. A harsh cease and desist letter might not only preclude an amicable outcome down the line but may also be bad PR for the company. And rather than protecting the brand, you may damage it. Remember the saying about flies and honey. A quick glance at chillingeffects.org reveals that a cease and desist letter has become something of a rite of passage on the Internet. But although they may be commonplace, well-considered letters can still go a long way.

If, however, the cease and desist does not work, then explore further. You should first read the terms of use of the site where you feel the brand is being harmed or misrepresented. It is easier to work within the provider's guidelines. For social networking sites, trademark and copyright infringement should be pursued first and foremost, as most often these are the clearest claims to make. Given the take down procedures that website holders have to abide by, all you need to prove is that the intellectual property is being infringed upon. However, there are several caveats. First, you must list the works that are being infringed, specifically giving the information on the work as well as the information and link to the work on the website.[16] Second, the complaint must be in good faith, which includes considering any fair use defenses before filing the complaint.[17] Once those options are exhausted to no avail, look further into what other actions you can take. Sometimes a more cost-effective approach is more PR and SEO than legal.

Whether you are watching or not, brands exist on the internet and in social media. It is better to join in on the conversation, build goodwill and make sure that the message is the message that is getting out there. Given the tools available, it is getting easier to keep vigilant watch and monitor a brand, for better or for worse. Tweet and Like away, comfortably knowing that you are the first step in brand management.

Endnotes

1. *See* American Marketing Association, Marketing Power, Dictionary, *available at* http://www.marketingpower.com/_layouts/Dictionary.aspx?dLetter=B.
2. The burden of policing one's brand has been held by courts in cases such as Tiffany, Inc. v. eBay, Inc., to be on the brand owner:

   > The Court is not unsympathetic to Tiffany and other rights owners who have invested enormous resources in developing their brands, only to see them illicitly and efficiently exploited by others on the Internet. Nevertheless, the law is clear: it is the trademark owner's burden to police its mark, and companies like eBay cannot be held liable for trademark infringement based solely on their generalized knowledge that trademark infringement might be occurring on their websites.

   576 F. Supp. 2d 463, 527 (S.D.N.Y. 2008), *aff'd in part*, 600 F.3d 93 (2d Cir. 2010). The Second Circuit agreed with the district court that Tiffany could not hold eBay contributorially liable based on generalized knowledge but rather must have been found to be willfully blind to the infringement. However, even though eBay conceded that it knew as a general matter that counterfeit Tiffany products were listed and sold through its website, both the district court and the Second Circuit concluded that without more than this, eBay did not have enough knowledge to trigger liability under *Inwood. Tiffany*, 600 F.3d at 110 *citing Tiffany*, 576 F. Supp.2d at 513-14 *and* Inwood Lab, Inc. v. Ives Lab, Inc., 456 U.S. 844, 102 S. Ct. 2182 (1982).
3. Brian Solis has been an outspoken proponent of businesses engaging the public in the social media forum as a brand marketing strategy, *see* "The Social Media Manifesto—Integrating Social Media into Marketing Communications," June 11, 2007, *available at* http://www.briansolis.com/2007/06/future-of-communications-manifesto-for/.

4. *See* Ty Inc. v. Perryman, 306 F.3d 509, 510 (7th Cir. 2002) ("The fundamental purpose of a trademark is to reduce consumer search costs by providing a concise and unequivocal identifier of the particular source of particular goods.").

5. There is no cure for "genericide." Once the mark becomes associated with a whole class of goods or services any challenge by a junior user wanting to remove a protection will succeed. See discussion, *infra,* at note 7. Therefore, it is important to communicate with the consuming public that a mark is not the product, i.e., it is not a q-tip that cleans ears, it is a Q-TIP cotton swab.

6. Bayer Co. v. United Drug Co., 272 F. 505 (D.C.N.Y. 1921). The court ruled that consumers had come to know acetyl salicylic acid by no other term but "aspirin" and therefore by granting a monopoly to the plaintiff, it would deprive the defendant as well as the trade in general "of the right effectually to dispose of the drug by the only description which will be understood." *Id.* at 514. For a further discussion of how to avoid genericism, *see* Charles R. Taylor and Michael G. Walsh, *Legal Strategies for Protecting Brands from Genericide: Recent Trends in Evidence Weighted in Court Cases,* Journal of Public Policy & Marketing, Vol. 21, No. 1, Social Marketing Initiatives (Spring, 2002).

7. Under Federal Statute, 47 U.S.C. § 230, Internet providers, such as Yelp!, who post content that is provided by another content provider, i.e., the site is not producing the content of the post, are immune from any liability based on the offending posts, except intellectual property infringements. Therefore, although a plaintiff may have a cause of action against the party that wrote and posted the defaming message, there is no action against the Internet provider that carries the post. *See* Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), *cert denied,* 524 U.S. 937 (1998) (the court ruled that Defendant was immune from any liability for distributing defamatory material on its website despite notice from Plaintiff of its defamatory nature), *cf.,* Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc) (the court concluded that the manner in which the service elicited information from users concerning their roommate preferences (dropdown menus specifying gender, presence of children, and sexual orientation without an option to not answer), and the manner in which it utilized that information in generating roommate matches (by eliminating profiles that did not match user specifications) meant that the defendant in fact created or developed the information claimed to violate the Fair Housing Act, and thus was responsible for it as an "information content provider").

8. *See* Rescuecom Corp. v. Google, Inc., 562 F.3d 123 (2d Cir. 2009) (The Second Circuit Court of Appeals vacated and remanded the district court's decision holding that Google's practice was a "use in commerce" of Rescuecom's trademark within meaning of the Lanham Act and therefore the district court would need to make a decision on whether this use was infringing or not.). However, as of March 2010, Rescuecom dismissed its lawsuit against Google claiming victory based on the fact that Google removed its trademark from the list of keywords, something Google may have done as early as 2005, and Google has instituted a policy to disallow the use of trademarks within the text of a sponsored link with some exceptions. But, in fact, what seems to be going on here is that Rescuecom is pursuing a separate litigation against Best Buy, the owner of the GEEK SQUAD mark, seeking a declaratory judgment that it is entitled to use the term "geek squad" as a keyword for a sponsored link which supposedly suggests comparative advertising. Therefore, a decision against Google might preclude the desired outcome against Best Buy. The bottom line then is that courts have ruled that selling keywords is a trademark use and comes under the Lanham Act, but we still do not know if this is an infringing use.

9. *See*, Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999) (where the appellate court construed a narrow interpretation of the use of metatags and initial interest confusion so that the words used in the metatag had to match the mark exactly in order to fit the brick and mortar model of putting a billboard on a highway). Therefore, success may not be assured when pursuing an initial interest claim against online infringers.

10. *See*, Taubman v. Webfeats, 319 F.3d 770 (6th Cir. 2003). In this case, the plaintiff sought an injunction of the original site, "theshopsatwillowsbend.com" and subsequently for the five ".sucks" sites that the defendant registered following the initial suit. The appellate court dismissed all these claims based on the fact that the defendant's websites were neither intended nor used for any commercial purposes and therefore the use of the plaintiff's mark was protected by free speech under the First Amendment as well as nominative fair use under the Lanham Act. The court further noted that even if there had been commercial use on these sites, there would still not have been a likelihood of confusion based on the fact that the defendant had clearly posted a disclaimer stating that his site was in no way affiliated with the plaintiff and moreover he provided a link to the plaintiff's site for those who had navigated to his site by mistake. The court did not find it dispositive against the defendant that he had engaged in negotiations to sell the domain name to the plaintiff because the defendant had no history of buying and selling domain names to trademark owners and moreover the negotiations were initiated by the plaintiff. *See also,* Bally Total Fitness Holding Corporation v. Andrew Faber, 29 F. Supp. 2d 1161 (C.D. Ca. 1998) (the court held that Faber had demonstrated that there was no likelihood of confusion based in part on the fact that the goods were not related and that a reasonable consumer would not mistake Faber's site for Bally's official site given that the defendant says his site is unauthorized and that he has superimposed the word "sucks" over the plaintiff's mark). *Cf.,* Shields v. Zuccarini, 254 F.3d 476 (3d Cir. 2001) (where the court held the defendant liable for likelihood of confusion for five of the domain names he registered that were very similar to the plaintiff's trademark due to the fact that he acted in bad faith with an intent to profit based on a lack of real content on these websites and a history of making a profit on these sites).

11. 47 U.S.C. § 230, see discussion, *supra,* at note 8.

12. Intellectual property claims are not protected by Section 230 immunity, so there is no blanket protection for Internet providers with regard to trademark and copyright infringement. However, one must consider for trademark claims whether the use is protected by fair use or the First Amendment, see discussion, *supra,* at note 11. And for copyright claims, one must consider the Digital Millenium Copyright Act of 1998 (DMCA), which offers a "safe harbor" to Internet service providers that meet all of the following criteria:

> A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—
>
> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in

which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

17 U.S.C. § 512(c). The issue of notification and expeditious removal has become a hot issue where copyright owners are trying to push the courts to define what this means exactly, *see*, Viacom International, Inc. v. YouTube, Inc., _ F. Supp. 2d _, 2010 WL 2532404 (S.D.N.Y., Jun. 23, 2010) (The court held that the defendant qualified for the safe harbor protection under the DMCA because it had removed any and all infringing videos that the plaintiff had specifically requested and moreover the defendant has instituted a policy of voluntarily removing posts that it feels may be infringing. It was not sufficient that the plaintiff made a general request to the defendant to remove all infringing videos, specific information was necessary.). It is important to note also that not qualifying for the "safe harbor" under the DMCA does not automatically mean that the Internet provider is contributorily liable for copyright infringement; this must still be litigated.

13. Lanham Act § 33(b)(4).

14. New Kids on the Block v. News America Publishing, Inc., 971 F.2d 302 (9th Cir. 1992) (fan site was allowed to use the plaintiff's trademark under a nominative fair use defense because there was no other way to refer to it).

15. See discussion, *supra*, at note 11.

16. *See*, 17 U.S.C. § 512(c)(1)(C) *and* Viacom International, Inc. v. YouTube, Inc., _ F. Supp. 2d _, 2010 WL 2532404 (S.D.N.Y., Jun. 23, 2010), see discussion, *supra*, at note 13.

17. *See*, 17 U.S.C. § 512(f):

Misrepresentations. Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

Courts, however, have been willing to allow complaints that were based on a subjective belief on infringement, even if that belief was incorrect. Rossi v. Motion Picture Ass'n of America, 391 F.3d 1000, 1004-05 (9th Cir. 2004).

Natalie Sulimani, as partner of Sulimani Law Firm, PC, is engaged in a wide variety of intellectual property, technology and general corporate matters with a strong focus on small businesses and entrepreneurs. Natalie is a frequent speaker and panelist on intellectual property, protecting your brand online and small business matters. You can follow her at www.twitter.com/sulilaw.

John S. Morales is an intern for Sulimani Law Firm, PC. and a student at New York Law School. John was formerly an Associate Editor at the International Trademark Association for its law journal, *The Trademark Reporter*. John is focusing his studies in law school on intellectual property.

Monitoring Your Employees: How Technological Changes Are Changing Employers' Ability to Manage and Control Their Workplaces

By Joel J. Greenwald

When a smart phone can send emails, take videos, surf the web, and even contain a GPS, it should be no surprise that technology provides employers with unprecedented means of monitoring employees. Of course, having a capability does not require using it, which means the question is no longer *can* an employer monitor its employees, but rather *whether*, *when*, and *how* it should do so.

Thoughtful and legally compliant employee monitoring can reduce an employer's exposure to both legal liability and business risk. Improper monitoring can create liability, such as for invasion of employee privacy. Making the correct use of employee monitoring is one of the key challenges facing businesses in the early 21st Century.

Why Monitor?

The reasons to monitor employees are the same as they have ever been:

- To prevent theft (including of trade secrets)
- To monitor employee disloyalty
- To improve productivity
- To avoid liability for employees' illegal acts

However, even if the reasons haven't changed, there's more urgency to them than before. Simply put, it is easier than ever for employees to steal—business information can be emailed or saved to a thumb drive with the push of a button. Furthermore, with employee tenure at historic lows, employee turnover (both voluntary and involuntary) at historic highs, and heavy use of outsourcing and consultants, social conditions make theft more likely; it's easier to steal from someone with whom you have little or no emotional connection, and in today's economy, many workers have little or no connection to the businesses that pay them.

Other forms of business risk have also been made more common by the advent of not just the Web but the advent of sites and applications that facilitate information sharing and interactive communication. For example, when almost everyone has an Internet presence—Facebook, LinkedIn, YouTube, MySpace, blogs, and Twitter—the risk of an employee publicizing something defamatory, discriminatory, or just plain unsavory about his or her employer or co-employees is enormous. It used to be, if you were an average private citizen, it took real effort to defame someone; now you can reach an audience of thousands or tens of thousands with a single post. In an interconnected, easily searchable world, the risk resulting from inappropriate posts falls not just on the poster, but on everyone connected with him or her—including the employer.

Monitoring Basics

Monitoring employees pits two different sets of legally recognized interests against each other: the employee's expectation of privacy vs. the employer's right to control its workplace. In balancing these interests, courts distinguish between an employee's work-related activities (which have little expectation of privacy) and an employee's private and personal activities conducted in the workplace (which carry a greater right to privacy).

Under federal law, employers can monitor the following:

- ***Activity on company-owned equipment*** for all communication: *e.g.,* URLs or email addresses contacted and time spent at each address or in the aggregate
- ***Content of business-related e-mail and voice-mail messages*** stored on company-owned equipment (such as a company server)
- ***Content of personal e-mail and voice-mail messages when there is legitimate business reason***, and *only* when the messages are stored on company-owned equipment

(Remember: state law may provide additional privacy protections beyond those of federal law. It's vital to always check applicable state and local law as well.)

One of the most critical points to remember in monitoring is that a company's reach is only as far as its own equipment. For example, a company generally cannot review the content of an employee's personal computer—unless there is a legitimate business reason to do so, and then after consulting an attorney.

What about the content of personal emails sent via a web-based account but from a company computer such as personal gmail or AOL mail? If they are captured by the company's equipment or network, those may potentially be viewable by the employer. If there was a policy in place which put staff on notice they had no expectation of privacy of such emails, then the chances are greater for such monitoring to be found to be permissible.

The Importance of Defeating Privacy Expectations and Defining Permitted or Appropriate Computer and Internet Use

It's important to "destroy" an employee's expectation of privacy. That is, if employees know they live in a

glass bubble, they have less right to complain when they are monitored. Well-thought-out, well-articulated policies can make the difference between being able to monitor employees or not. For example, an email / Internet policy should state:

- All email sent from company machines is the property of the employer (even emails from personal accounts), and there is no expectation of privacy
- The employer has the right to monitor Internet and email usage
- Offensive or harassing emails, messages, or postings are prohibited
- Computer and company email access are for business, not personal use, and improper usage may subject employee to discipline
- Passwords to company equipment must be kept private and not made available to others (except to the extent IT may need them)

Not only does a policy like this lay the groundwork for computer monitoring, it also makes it plain to employees that certain behavior is inappropriate and can lead to discipline or termination.

However, since it's important to "never give an order you know won't be followed," employers may want to outline limits for personal use. Everyone, no matter how responsible, makes *some* personal use of office computers and Internet. Unless an employer actually intends to discipline people for checking Facebook on their lunch hour, it's better to allow modest, reasonable personal use of company technology (i.e., during lunch). This lets an employer have a credible and enforceable technology policy.

It's vital to get signed acknowledgement of the policy; this makes it clear that the employee was aware of and agreed to it as a condition of employment. These acknowledgements should be kept in the employees' personnel file, since in the event of litigation, they could be critical.

Don't Interfere with Attorney-Client Privilege

Even when there is no expectation of privacy, employers may *not* read communications with an employee's attorney. That was the holding in the recent New Jersey case of *Stengart v. Loving Care Agency, Inc.*[1] The state Supreme Court held that notwithstanding that the emails were relayed by company equipment and were readily accessible by the IT department, the attorney-client confidentiality privilege trumped the employer's computer monitoring policy. Since it's reasonable to believe that other courts will come to the same conclusion, employers should be careful to not read employee correspondence with counsel.

Phone Monitoring: Permissible Within Reason, in Line With a Policy

As with computer or Internet-use monitoring, phone monitoring is allowable in certain circumstances. This depends on whether the company has a policy putting employees on notice of monitoring. With advance notice of a proper phone-monitoring policy, any business call on company lines can be monitored (or listened-in on) by the company, and can likely be recorded (keeping in mind state laws that may require notice to the caller).

On the other hand, personal phone calls on company equipment can be monitored only long enough to determine that they are personal calls. Once that's determined, the company may no longer listen in—though it may take note of the fact that the employee is on a personal call and the call's duration. If employees are on notice that they may only make reasonable numbers of personal calls, or only make them at certain times, they can be disciplined or terminated for excessive personal phone use—just as they can be terminated for excessive personal use of computer equipment.

As with computer and Internet policies, phone-usage policies should be in writing. They should explicitly destroy any expectation of privacy, permit monitoring, and ban certain use (e.g., discriminatory, harassing, defamatory, or criminal use; or excessive personal use). The company should get a signed acknowledgment of receipt from all employees.

Also, applicable state and federal laws must be complied with. For example, New York and New Jersey only require "one-party consent" to record phone calls, which means that if the employer allows monitoring or taping, it may do so without the consent of the person on the other end of the phone line. However, some states require two-party consent, and in those states, monitoring or recording a phone call without the concurrence of all parties to the call could be a criminal act. Therefore, if making out-of-state calls to customers, etc., you should have a taped disclaimer of your intent to record or monitor the call, should you decide to do so.

Smile: You're on Employer Camera

Within some fairly broad limits, it is possible to use video surveillance in the workplace—though as with phone and computer monitoring, the company should have a written policy putting employees on notice of surveillance and destroying any expectation of privacy.

What CAN you do with video surveillance?

- Monitor public areas

What CAN'T you do with video surveillance?

- Monitor restrooms, locker rooms, changing rooms, fitting rooms, or guest rooms (e.g., in a hotel)
- Record sound
- Monitor a unionized workforce (may violate the collective bargaining agreement or otherwise be an "unfair labor practice")

- Selectively monitoring—this could give rise to a claim of discrimination

Video monitoring can be valuable, but it can also be trickier to implement properly than other kinds of monitoring. Depending on your industry, however, this can be a valuable tool, for example, to monitor inventory.

Where, Oh Where, Have the Employees Gone?

GPS allows real-time monitoring of location. For example, if a car or truck is outfitted with GPS, it's possible to know where it is at any given moment. Can employers use this tool to know whether deliveries are being made, or the whereabouts of employees, by installing GPS in company-supplied or –owned vehicles?

Yes.

As with other forms of monitoring, employees should be put on notice of the potential for monitoring. And while it's acceptable to monitor location during work hours, it should not be used to track employees during off-duty hours.

What About What Your Employees Say Online?

Many employees feel that employer restrictions on what they say is a violation of First Amendment free speech rights. They're wrong—private-sector employees have no free speech rights against their employers, since the First Amendment restricts government actions only.

Employees can hurt their employers with online posts a number of ways. One, of course, is by giving away confidential information—and not always deliberately: an employee blogging or posting about projects he's working on could give away critical product development or marketing information.

Other possible ways online posts could hurt a company include the employee making racist or otherwise discriminatory remarks, which could be imputed to the employer; or if the post defames someone. (If the post defames the company, the company may be able to sue the employee for defamation.)

Never before has any and every person had the ability to publish to an audience of thousands or even millions with the push of a button. Contrary to popular wisdom, words *can* hurt you—they can lead to liability, such as for defamation or discrimination; or they can cost a company business or its good reputation. It, therefore, may be incumbent on employers to monitor their employees' social media activities, blogging, and other online publications.

However, be careful! While anything posted on a public site or forum is public, material on a private, password-protected, or access-by-invitation-only site is not. Employers should never access those sites, even if they obtain the password or other access. Also, they should be careful with how they deal with information regarding employee membership in protected categories or groups (such as religion, race, national origin, or family status), which could lead to discrimination claims.

The Necessity for Fair, Policy-Driven Monitoring

With computers making the instant transmission and publication of information possible, the potential for employee mischief, misdeeds, or costly mistakes is high. Information can be stolen, or negligently disseminated, in an eye-blink. Work time can be wasted more easily than ever. And because it's a small, highly searchable world online, it's easy to associate an employee—and what he or she says or does—with his or her employer. For all these reasons, it's vital that companies monitor their employees' computer, Internet, and also social media (at least, publicly available social media) activities.

Similarly, in regard to monitoring employee phone calls, or using GPS or video surveillance, social and economic forces are decreasing employee loyalty. Since the means exist to monitor employees in these ways, companies need to at least consider doing so.

While monitoring, employers need to recognize that employees, even at-will employees, have certain privacy and other rights that employers must respect. It's necessary to strike the right balance between employer and employee interests. While employers would be prudent to consult with their employment lawyers regarding their particular situations or local laws applicable to their business, one of the best ways to do that is by having computer-use, phone-use, and monitoring policies in place, so that employees know what is expected of them and what actions their employer may take. Having proper policies may help reduce legal concerns growing out of employee privacy expectations. It's also the better way to run a business, since it's only fair to let employees know what's allowed, what's not, and what the consequences may be. However, a failure to utilize these monitoring tools may result in lost business, stolen clients, and employee time-wasting that could otherwise have been prevented. Used appropriately, employee monitoring can help protect businesses from disloyal and disgruntled employees.

Endnote

1. 201 N.J. 300 (2010).

Joel J. Greenwald, Esq., is the managing partner of Greenwald Doherty, LLP, an employment and labor law firm, representing exclusively management, and can be reached at (212) 644-1310 or jg@greenwaldllp.com.

The FACTA Red Flags Rule—For Lawyers

By Kristen Mathews and Scott Carpenter

Introduction

As technology has advanced to facilitate compiling, transferring and sharing personally identifiable information, so too has it augmented the risk of identity theft to consumers. Accordingly, federal and state governments have placed ever-increasing privacy and data security obligations on entities that maintain personal information. As one such response, Congress passed Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA) calling upon the federal banking regulators and the Federal Trade Commission (FTC) to provide guidelines for the identification of possible instances of identity theft.[1]

On October 31, 2007, the FTC and the federal banking agencies promulgated the final regulations, now known as the "Red Flags Rule," requiring covered entities to design and implement Identity Theft Prevention Programs that identify and detect Red Flags signaling possible identity theft.[2] Under the Red Flags Rule, companies establishing such programs must create policies and procedures not only to recognize and detect Red Flags, but also to respond to Red Flags by preventing or mitigating potential identity theft.[3]

The FTC has continued to postpone its enforcement of the Rule due to confusion and uncertainty as to what entities are subject to the FTC's jurisdiction. But before delving into the scope of the Red Flags Rule it is helpful first to understand what exactly the Rule requires.

Identity Theft Prevention Programs

As stated above, under the Red Flags Rule, covered entities must develop written policies and procedures to identify and detect Red Flags, as well as respond to Red Flags by preventing or mitigating potential identity theft. A Red Flag is a pattern, practice or activity that could indicate identity theft. An important rule of thumb for any Identity Theft Prevention Program is that it must be tailored to a specific business. One size does not fit all. A Red Flags program therefore must reflect the size and complexity of a covered entity and the nature and scope of its activities, and thus the Red Flags incorporated into a program must be derived from those very same factors.

Because covered entities must tailor their Red Flags programs to their particular business, these companies will need to do risk evaluation to assess current identity theft prevention measures, their shortcomings and the risks to customers. Risk factors include: (1) the types of covered accounts a company offers or maintains, (2) the methods a company provides to open its covered accounts; (3) the methods a company provides to access its covered accounts; and (4) a company's previous experiences with identity theft.[4]

Given the broad reach of the regulations, the agencies gave businesses significant flexibility to determine which Red Flags are relevant to their business to detect identity theft. Also, to assist covered entities in choosing which Red Flags to identify, the federal regulators provided a list of 26 possible Red Flags that may require further action when they come to the attention of a company, consisting, in part, of the following:

- A fraud alert, credit freeze, or address discrepancy is included with a consumer report or provided by a credit reporting agency.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer.
- Documents, applications, or photo identification provided appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.
- Other information on the identification is not consistent with readily accessible information that is on file with the covered entity, such as a signature card or a recent check.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the covered entity.[5]
- Personal identifying information provided is not consistent with personal identifying information that is on file with the covered entity.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account.

While a covered entity will not need to justify to a federal agency its failure to include in a Red Flags program a specific Red Flag from the list of examples, "a covered entity will have to account for the overall effectiveness of a program that is appropriate to its size and complexity and the nature and scope of its activities."[6] Therefore, it is vital that a company's program be specifically tailored to the types of identity theft risks its customers are exposed to by virtue of the company's products or services.

Once a covered entity has identified relevant Red Flags, it must create policies and procedures to detect and respond to them. In particular, a Red Flags program should address the detection of Red Flags in connection with the opening of covered accounts and access to existing covered accounts. In general, detection will require sound controls and staff training to ensure that a company recognizes and addresses Red Flags of identity

theft. And to the extent a company has the technological resources to assist in detection of red flags (i.e., monitoring transactions for unusual account activity), a company should include such resources in its program. The Rule, however, is purposefully broad enough to provide companies the flexibility to tailor policies to the specific risks they face.

Since not all Red Flags relate to actual instances of identity theft, a company's response to a Red Flag should be commensurate with the degree of risk posed. Not only must companies assess whether a Red Flag does or does not evidence a risk of identity theft, but also they must have policies and procedures in place to respond appropriately to the Red Flag depending on the risk involved. Companies also may need to consider certain aggravated factors that indicate increased risk to consumers, such as a data security incident that results in unauthorized access to a customer's account records or a notice that a customer has been victimized by a "phishing" scheme.[7]

Finally, under the Red Flags Rule, companies must acquire approval of the program from the board of directors or a committee of the board, as well as exercise oversight of the implementation of the program, training staff and employees, and service provider arrangements.[8] Furthermore, companies must continuously update their list of Red Flags.[9] With changes in technology, some Red Flags that are relevant to current industry risks may be obsolete in a few years.

To be sure, the Red Flags Rule requirements are not inconsequential. The creation and implementation of an effective Identity Theft Prevention Program requires careful analysis, planning and oversight. The FTC has provided businesses with some tools and guidance regarding the Rule, presumably to help ease the burdens on companies. To date, the FTC has provided a how-to guide for businesses, FAQs, and an Identity Theft Prevention Program template for low-risk entities.[10] Nevertheless, there has been and continues to be confusion and conflict as to what entities are covered under the Rule. And such issues have spilled over into the courts and halls of Congress.

The Scope of the Red Flags Rule

The Rule applies to "financial institutions" and "creditors" that maintain "covered accounts." While at first glance that may not seem like a expansive universe of covered entities, the Red Flags Rule, as set forth by the FTC and the federal banking agencies, applies broadly. Many companies that considered themselves to be neither financial institutions nor creditors, therefore, were caught off guard by the far-reaching scope of Rule as interpreted by the federal regulators.

The definition of "covered account" is divided into two parts: (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.[11] In the commentary to the Rule, the federal regulators express their belief that small business accounts and sole proprietorship accounts may be vulnerable to identity theft, and, therefore, should be considered for inclusion in a covered entity's compliance with the Red Flags Rule.[12] However, because the Rule is flexible and risk-based, a covered entity may determine which business accounts, if any, to include in its program. An account, though, must be a continuing relationship, and thus, single transactions are not covered under the Rule.[13] Hence, examples of a single transaction that would not create an "account" include the purchase of a money order, one-time prepaid card (e.g., gift card), or goods or services that are paid for at the time the goods are transferred or the service is rendered.

Financial institutions are defined in accordance with the Fair Credit Reporting Act (FCRA) to include banks, mortgage lenders, savings and loan associations, mutual savings banks, credit unions and any other person that, directly or indirectly, holds a "transaction account" belonging to a consumer.[14] A "transaction account" means as "a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others."[15]

Much of the Red Flags controversy, though, has revolved around the definition of creditor. Creditors are defined as persons or businesses that regularly arrange for the extension, renewal, or continuation of credit.[16] "Credit" means "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment thereof."[17] The Rule lists a range of entities covered under the definition of creditor, such as finance companies, car dealers, utility companies, and retailers offering financing. The FTC has indicated, however, that many more entities are covered.

The FTC, according clarifying statements, has taken a bright-line approach as to the types of businesses covered as creditors. For instance, in an October 2008 Enforcement Policy Statement, the FTC asserted that "any person that provides a product or service for which the consumer pays after delivery is a creditor."[18] Thus, under this broad interpretation, many companies that permit their customers to defer payment for any purchase, and do not require payment when goods or services are provided, may be covered under the Rule. Consequently, the FTC cast its net far and wide to cover entire industries neither ordinarily considered creditors nor ordinarily subject to the FTC's jurisdiction, most notably lawyers and law firms.

The FTC's Attempt to Regulate Lawyers

Perhaps the least likely way a lawyer would describe his or her practice would be as providing credit. According to the FTC, however, lawyers that bill their clients for past services on a periodic basis, rather than requiring up-front payment, fall under the definition of creditor.[19] Lawyers, law firms, and bar associations including the American Bar Association (ABA) protested, claiming that Congress did not intend to regulate the practice of law, the application of the Rule to lawyers exceeded the FTC's authority under the FACTA and the FTC's interpretation would impose significant burdens on law firms.

In light of failed efforts to convince the FTC otherwise, the ABA sought an injunction and declaratory judgment in a U.S. District Court for the District of Columbia finding that lawyers are not covered by the Rule. Specifically, the ABA argued that the FTC's interpretation of the Rule was "arbitrary, capricious and contrary to law," and that the FTC failed to set forth "a rational connection between the practice of law and identity theft; an explanation of how the manner in which lawyers bill their clients can be considered an extension of credit under the FACTA; or any legally supportable basis for application of the Red Flags Rule to lawyers engaged in the practice of law."[20]

On October 30, 2009, Judge Reggie Walton in *American Bar Association v. Federal Trade Commission* ruled from the bench in favor of the ABA that the FTC exceeded its authority by applying the Red Flags Rule to lawyers and law firms.[21] And while the FTC is appealing the decision, other industry groups, such as the American Medical Association and the American Institute of Certified Public Accountants, have filed suits similar to the ABA's seeking exemption from the Red Flags Rule.

In late May 2010, given the continued confusion regarding the scope of the Rule, the FTC (for the fourth time) delayed enforcement, this time until December 31, 2010.[22] According to the FTC, Congress requested the delay to consider legislation that would limit the scope of entities covered by the Rule. As FTC Chairman Jon Leibowitz stated, "Congress needs to fix the unintended consequences of the legislation establishing the Red Flags rule—and to fix this problem quickly. As an agency we're charged with enforcing the law, and endless extensions delay enforcement."[23] One proposed bill would exempt from the definition of creditor certain businesses (with under 20 employees) engaged in health care, accounting, and the practice of law, as well as a catch-all for other low-risk entities if they apply to the FTC for exemption.[24]

Conclusion

While the FTC's announcement that it will delay enforcement does not affect other federal agencies' ongoing enforcement of the Rule as it relates to financial institutions and creditors subject to their oversight, it remains unclear, however, at the time of this writing, what Congress ultimately will do to clarify the scope of the Red Flags Rule.

Endnotes

1. 15 U.S.C. § 1681m(e).
2. 72 Fed. Reg. 63,718.
3. 72 Fed. Reg. 63,719; *see* 16 C.F.R. § 681.2(d).
4. *See* 16 C.F.R. Appendix A to Part 681.
5. For the complete list of Red Flags see, for example, 16 C.F.R. Supplement A to Appendix A to Part 681.
6. 72 Fed. Reg. 63,732.
7. *Id. at* 63723.
8. *Id. at* 63730.
9. *Id.*
10. *See* Fighting Fraud with the Red Flags Rule: A How-To Guide for Business, *available at* http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.
11. *See* 16 C.F.R. § 681.2(b)(3).
12. 72 Fed. Reg. 63,721.
13. *See* 16 C.F.R. § 681.2(b)(1).
14. 15 U.S.C. § 1681a(t).
15. 12 U.S.C. § 461(b)(1)(C).
16. See 15 U.S.C. § 1691a(e).
17. See 15 U.S.C. § 1691a(d).
18. *See* FTC Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.2, *available at* http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf.
19. *See* The Red Flags Rule: Frequently Asked Questions, *available at* http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm.
20. *See* American Bar Association Complaint, *available at* http://www.abanet.org/media/nosearch/1_1_Complaint.pdf.
21. *American Bar Association v. Federal Trade Commission*, No. 09-1636 (D.D.C. October 30, 2009).
22. *See* FTC Press Release, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule, *available at* http://www.ftc.gov/opa/2010/05/redflags.shtm.
23. *Id.*
24. S. 3416, 111th Cong. (2010).

Kristen J. Mathews is head of Proskauer's Privacy and Data Security Group and a member of the Technology, Media and Communications Group. Kristen focuses her practice on technology, e-commerce and media-related transactions and advice, with concentrations in the areas of data privacy, data security, direct marketing and online advertising.

Scott J. Carpenter is an Associate in Proskauer's Washington, DC office. Scott has advised clients from numerous industries on a wide array of state and federal privacy laws and regulations. He has considerable experience counseling clients regarding the complex provisions of the Fair Credit Reporting Act (FCRA) and the FTC's Red Flags Rule, in compliance of which Scott has drafted numerous Identity Theft Prevention Programs.

Taking Control of E-Discovery: Managing Internally and Consistently

By Cynthia Bateman and Kenneth C. Koch

Litigation expenses, specifically the costs associated with e-discovery, make up the lion's share of corporate law department budgets. Even an organization with minimal litigation can suffocate under the cost of e-discovery in one unexpected lawsuit or regulatory investigation. Additionally, the organization that does not drive process consistency and repurpose knowledge across all matters in its litigation profile may face more than out of control costs; it faces the risks associated with e-discovery non-compliance, including monetary sanctions, adverse inferences and damage to reputation, not to mention too many sleepless nights.

Taking control of your organization's e-discovery can be a challenging exercise. Yet, the cost of planning—in terms of time, dollars and effort—can be a fraction of the cost of a single e-discovery crisis. For the company that's not ready, the potential for e-discovery risk and overspending recurs each time a new lawsuit or regulatory action comes through the door.

Your organization can mitigate that risk and accomplish reasonable, good-faith e-discovery compliance by creating defined, consistent e-discovery processes; identifying the right internal and external resources to execute those processes; locating the proper technologies that fit your organization's e-discovery needs; and tracking e-discovery metrics to assist in forecasting budgets for individual matters and to gain visibility into your annual e-discovery spend.

Why Is E-Discovery So Expensive?

It's no secret that attorney review costs typically represent the single largest line item for virtually every matter's overall discovery spend. Still, the discovery process begins long before reviewers take their seats to tackle hours of tedious multiple passes through data to determine relevance, privilege and dozens of other attributes to eventually assemble the pieces of the puzzle. Decisions made through the first half of the industry-accepted e-discovery workflow (Figure 1), impact the cost of each pair of attorney eyes and how many hours those eyes are devoted to reviewing documents.

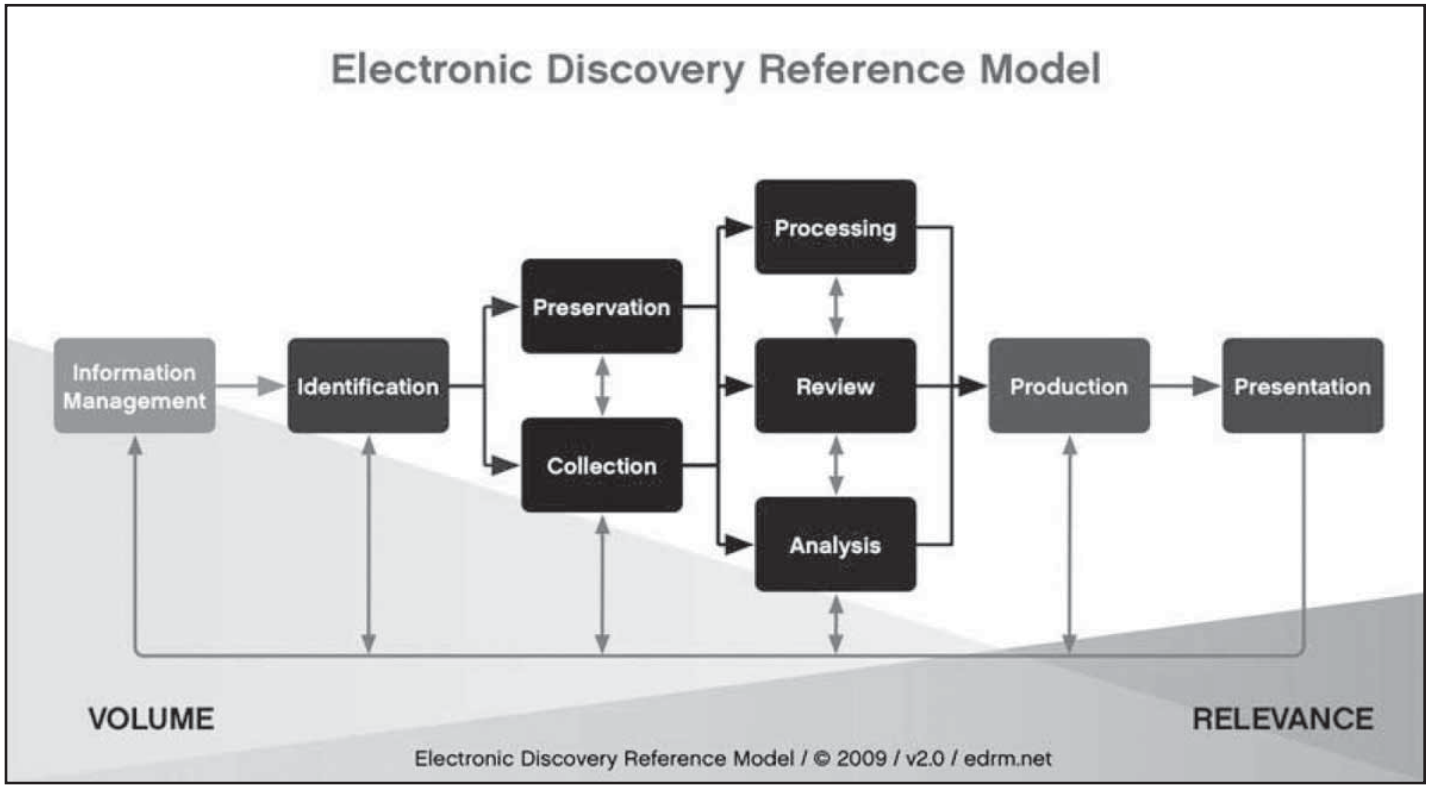


Figure 1: Electronic Discovery Reference Model (EDRM)

Even though outside counsel is generally involved in early decisions surrounding the identification, preservation and collection of potentially relevant information, in-house counsels often are the first to hear the preservation alarm go off. Subsequently, they are immediately thrown into the process of finding the right people and the right systems, issuing the right legal-hold instructions at the right time, tracking down the right IT resource to achieve collection of the right data, and engaging the right service providers to process, host and produce. For fear of collecting too much or too little, they typically then hop from data source to data source in search of what will satisfy a reasonable, good-faith effort. Take these same case-specific reactive needs—identification, preservation and collection—and multiply them across dozens, hundreds or even thousands of new matters, and then assign them to dozens or hundreds of in-house attorneys and support professionals, and then engage dozens or hundreds of outside counsel across these matters to represent your interests. Cases are always unique; facts, claims and defenses warrant creative legal strategies, which can be different in every matter. However, the *processes* of identification, preservation, collection, production, review, analysis and production—and documentation of the process actions taken—can be planned, deliberate and consistently applied. A healthy dose of e-discovery process planning can help control e-discovery overreaction costs, thereby helping your organization avoid the expense of over-collection that can ultimately result in attorney time spent reviewing irrelevant data.

Excessive Costs Do Not Necessarily Mitigate Risk

By its very nature, lack of process consistency can not only increase the costs of discovery across matters, it can also increase the risk of counsel in different jurisdictions making conflicting representations regarding data accessibility, data availability, normal-course records management practices, and preservation and collection methodologies. Again, planning and embedding consistent discovery processes across in-house and outside counsel can help mitigate these risks as well as improve your ability to control and protect company information assets spread across a variety of service providers and law firms. These providers may have your information stored on their servers for years until final matter resolution, and proper control and disposition processes will help ensure that matter resolution procedures including vetting of additional preservation obligations are addressed before data is ultimately deleted.

The First Stride Is the Longest

Proactively addressing e-discovery can seem like a daunting exercise for in-house counsel, particularly when they have little to no time to step back and thoughtfully evaluate what needs to be done. Very few in-house attorneys have the luxury of time for such proactive initiatives while in the midst of managing a case load, providing day-to-day advice, and working toward fulfilling the corporate mission. Yet, taking the time and resources to look at what is in place, identify what works, where the risks and gaps reside, and developing a prioritized plan for addressing those risks is a necessary first step before building a plan for e-discovery response.

A thorough e-discovery assessment should include an objective evaluation of all processes in place for the EDRM workflow. This comprises documentation of processes, internal and external resources used to execute processes, enabling technologies and tools, and the controls in place to address changes to the organization, including mergers and acquisitions, hardware and software investments, and personnel or cultural shifts that could require adjustments to discovery process. Notably, e-discovery assessments and risk evaluations should be performed relative to each individual organization's industry, business complexity, litigation profile and discovery intensity. For example, discovery risk for a large pharmaceutical corporation may not look anything like discovery risk for the small software developer. Therefore, meaningful assessment findings and prioritized recommendations should be relevant to each organization's circumstances.

The Right Team

Control resides in accountability, and sound e-discovery readiness involves assignment of the appropriate resources. Resources include those who own responsibility for the overall program and help ensure a consistent, strategic approach to the discovery process. Resources should also be assigned to take on individual matter responsibilities for shepherding the documents through the process to completion while properly documenting case-specific decisions made and actions taken.

Typically, effective strategic e-discovery teams are multidisciplinary and include internal constituencies from legal, information technology, information security, and records management. Companies with hundreds to thousands of cases may assign full-time resources from each of these groups, but plenty of organizations have personnel who are responsible for e-discovery strategy and tactical response in addition to other duties. The essential key is ownership, and providing a centralized person or team of people who can provide consistent process guidance and share knowledge among all the stakeholders. For your organization, ownership could reside in any number of options—an E-Discovery Manager, E-Discovery Counsel, an entire E-Discovery Advisory Board, a Senior Paralegal or a Project Manager. It is not as much about the title as it is about having the right person or people in place. There is no room for apathy in the world of discovery response.

A smattering of global organizations have litigation profiles that warrant in-house staffing, hardware and software sufficient to provide full EDRM support, including the entire suite of processing, data hosting, review attorneys and production services. The large majority of companies, however, rely on external providers to support these functions, augment their in-house capabilities with subject matter professionals, and continuously improve the technologies that enable quality data processing and efficient attorney review. Typically, the worst time to find external service providers, whether consultants, data collection or data processing vendors, is after a lawsuit has been filed and the company has to "react" its way through the e-discovery maze. Consider investing time before the next event trigger to survey the market and evaluate provider capabilities and product features, and identify one or two candidates who are a good fit for your organization's needs. This exercise in readiness should provide comfort around knowing who stands ready to help when the time comes. More importantly, your organization and the service provider should have an up-front understanding of pricing, service levels and turn-around times, all of which will help you forecast discovery budgets and make proper representations to your adversary about data availability, production timelines and the like. The more experience with preferred provider relationships, the more control an organization can have over the costs of discovery. The provider should know your company, your data, your people, your culture and your processes; be able to repurpose knowledge of your infrastructure and systems across matters; and be able to readily react to your needs with little to no learning curve as new matters arise. Finally, consistently using an established external service provider can facilitate continuity across matters where the organization is represented by various outside counsel firms, expert witnesses and other advisers.

Sound e-discovery plans and the professionals supporting them should be flexible enough to accommodate change and focus on continuous improvement. New case law and the evolving federal, state and local rules governing discovery require companies to adapt quickly, while at the same time businesses are constantly introduced to disruptive technologies that claim to drive productivity and increase revenue. Consider building your e-discovery program with people who can address the risks and challenges associated with identifying, preserving and collecting potentially relevant information and data that can be created or stored in the latest technology *before* the software purchase contract is signed. E-discovery risk cannot be the tail wagging the dog of increased employee productivity and revenue generation, but having e-discovery resources in place to proactively evaluate the impact of such a purchase and mitigate potential risks in advance of implementation can save considerable hours and dollars.

The benefits gained by having consistent processes around e-discovery can be considerable. Most notably, the company will likely have an increased confidence in responses to document requests and can help counsel manage the risk of missing key information.

The Power of Visibility

It may be possible to count on one hand the number of in-house attorneys who would answer the question, "How much do you spend annually on e-discovery?" with something other than, "Your guess is as good as mine." Other than anecdotal horror stories of that one matter where the discovery costs exceeded the company's potential liability in the case by several fold, many organizations have very little in place to track discovery-related spending. While the LEDES® Oversight Committee has posted on the Uniform Task-Based Management System Website its plans to release new UTBMS billing codes specifically for e-discovery activities later this year, e-discovery efforts usually require resources in addition to outside counsel, the only providers required to bill with UTBMS. Ideally, visibility into the full e-discovery spend should include the costs of all internal resources and external service providers engaged to accomplish all steps in the EDRM. It is tough to control costs if one cannot first quantify what they are.

To quantify e-discovery spend, first identify those data points that will need to be captured. Focus initially on those with the bigger "bang," such as collection volumes, per gigabyte processing costs, attorney review rates, and review decisions per hour. Then, become more detailed and sophisticated in your tracking and include elements such as throughput (time from identification through production), filter and culling rates, average document and page counts per gigabyte, average collection volumes per custodian, and more.

Data can be gathered and managed in simple spreadsheets or advanced dashboard software, both of which can provide graphic representations and multiple views of your information, so that you may identify and target high cost areas. Dashboards can be configured to provide custom slices of data, including individual matter spend, costs attributed to a specific type of litigation, cases in a single jurisdiction, or aggregate discovery expenses over all matters in a given period of time.

Pay for What You Need, Shift What You Don't

The ability to execute a defined, methodical discovery process and provide visibility into the costs associated with each of the EDRM steps as described above can place an organization in the favored position of control. All of the data points captured can be used in a model that will help to quickly and accurately estimate response costs. Should an adversary make unreasonable discovery

demands, this model and corresponding knowledge of the costs associated with responding can be used to help negotiate a fair and reasonable scope of discovery, and perhaps eventually shift some of the response costs to the other party.

Demonstrating Value

Companies make investments based on potential ROI and investments in e-discovery readiness and response are no exception to that rule. In today's economy, belts are tighter and leadership is often wary of proactive, discretionary spending, particularly on those projects that do not have a direct monetary return. Consequently, how can in-house counsel articulate the need to take control of e-discovery and demonstrate value to the organization?

- First, organizations with reasonable, good faith, consistently-applied discovery processes help drive consistency across matters, which in turn help prevent the same work being reinvented time and time again across matters by different outside counsel.
- Second, the sheer nature of today's e-discovery process—particularly in light of federal, state and local rules requiring meaningful, early e-discovery negotiations with an adversary—seems to suggest that whoever is more reasonable may be more likely to win. A fully developed process for addressing identification, preservation and collection of potentially relevant information can give the court and an opponent a clear view of what you are willing to do, what you consider to be outside a reasonable scope, and a fair estimate of associated costs. Transparency into the nuts and bolts of the EDRM workflow as it applies to a case can help avoid expensive, protracted discovery disputes and move along to the business of matter resolution.
- Third, companies who build internal competencies and develop experience with e-discovery may reduce or eliminate the need for outsourcing in one or more steps of the EDRM. Full program development, including a focus on advanced training and technology, may allow an organization to reduce its reliance on vendors. Those who prefer to outsource can still realize significant cost avoidance and increase efficiency by establishing preferred provider relationships and repurposing knowledge from case to case.
- Fourth, as one begins to implement and embed a formal e-discovery program and gather information surrounding the data points and cost metrics, one can create a fuller picture of the case-specific and overall spend. Trends will likely emerge which may afford the ability to focus on areas of high cost and inefficiency and further refine and quantify e-discovery expenses. Having the means to rapidly project cost for a given request or demand based on real, historical data can help the company articulate the burden associated with requests and enhance its ability to negotiate reasonable alternatives with opposing parties.
- Finally, the cost of planning is relatively low compared to the typical time and expense of dealing with an e-discovery crisis, not to mention crisis after crisis. Planning ahead can help increase efficiency of response in an effort to eliminate the "fire drill." There is no silver bullet e-discovery solution, nor is there a program that is 100 percent risk free.

There will likely be situations where the plan will have to be adjusted and legal strategy will dictate what is done in each case. A fully developed discovery program, managed internally and consistently across matters, however, can provide a reliable process framework, lead to lower risk and exposure, and help an organization realize measurable cost savings.

Kenneth C. Koch is a principal and Cynthia Bateman is a director in KPMG LLP's Forensic Technology Services practice. In addition, Koch leads KPMG LLP's Forensic Technology Services Practice in the Southeast Area of the United States.

KPMG LLP, the audit, tax and advisory firm (www.us.kpmg.com), is the U.S. member firm of KPMG International Cooperative ("KPMG International"). KPMG International's member firms have 140,000 professionals, including more than 7,900 partners, in 146 countries.

This article represents the views of the authors only, and does not necessarily represent the views or professional advice of KPMG LLP.

A How-To Guide for Negotiating Tech Deals

By Mark Grossman

I started my career in a mid-sized law firm doing sophisticated corporate deals about 28 years ago. Just over 20 years ago, my practice evolved into doing sophisticated tech, telecom and outsourcing deals. With this evolution, I found new contracting norms. The most significant was that I went from a world of good first drafts of agreements prepared by competent lawyers to a world where first drafts often came from illiterates. This article is a how-to guide to get you from illiteracy to a workable and fair agreement.

Unfortunately, sales teams dominate my tech deal world and they think a good contract is the last one they did with just the names changed. After all, that's the easiest path to a commission check this quarter.

I would comment that most first drafts from tech vendors (including brand-name vendors) are atrociously written. They arrive on thoughtlessly used templates modified by the incompetent. They are not so much one-sided in favor of the vendor as simply not an expression of the deal.

The norm in my world is that after my first pass on a proposed agreement I will have 5 to 15 comments and redlines per page. Now, consider a hypothetical 30-page agreement (without attachments), and simple arithmetic tells you that we have 150 to 450 issues to discuss with the vendor.

Some of the discussion is substantive like discussing intellectual property, indemnification, or carve-outs to the limitation of liability. Much of the discussion is about defining core business terms like what the buyer is buying and what it will cost. (If you think tech agreements couldn't possibly leave out core terms like this, you don't live in my tech deal world.) Finally, a lot of the discussion is about rewriting our way through the illiteracy of the first draft. In this category, many of my comments consist of, "What does this mean?"

What Are the Goals?

I think that it is important that we define the goals for the negotiation of our hypothetical deal. For most deals, I define the goals this way.

Let's start by imagining that everyone sitting at the negotiating table is not available to interpret the agreement when a question arises. The written document has to be good enough to stand on its own. It must explain the deal sufficiently such that a substitute team with the same training as the original negotiating team can understand the intention of the parties.

The underlying point, beyond the obvious goal of avoiding the need for parol evidence to foster interpretation, is that tech contracts don't need to define every complex tech concept in such a way that a hypothetical high-school-educated juror could interpret it. Rather, the assumption is that interpretation would be by a team capable of understanding a technical contract and could dumb down the explanation as needed.

Another goal is simply to use the contracting process to ensure communication between the parties. I still find it amazing when I start probing a description of services only to discover that the parties have so few overlapping ideas on what the contract is about. Then, when they do agree, I find myself often saying: "That's great and we agree, but the contract does not say that. Can we reword it to simply say what you just said?" (All the while, I can feel the sales team seething at me because of my absurd requirement that the contract accurately state the deal.)

Lastly, I think another goal should be to pull those one-sided vendor terms back to the middle. Thus, you need to focus on things like limitations of liability, indemnity, choice of law, acceptance testing procedure, and so on.

Norms in the Industry

The tech world has some rather firmly established deal norms. It's important to know those so you don't push where pushing is not likely to garner meaningful concessions. Knowing the norms allows you to effectively focus on the areas where you can have impact while choreographing your concessions around areas where you're not likely to win the battle anyway. You simply cannot negotiate these deals effectively unless you understand the norms.

For example, the IT world has developed some unusual norms with warranties and allocating risk. In other industries, these might seem absurd, but not in IT world.

As a preliminary matter, let's clarify that I'm using the broad term "IT" in a broad sense. The same principles would apply whether we're discussing outsourcing your entire IT department, hiring somebody to design a website for your company, buying hardware, or just having some software customized for your company. Whatever it is, many of the same contracting norms apply.

Warranties

If your new car doesn't work, you take it to the dealer for repair. Knowing what it's supposed to do is easy. After

all, it's a car. Everybody knows what a car's supposed to do.

It's rarely that easy with IT-related contracts. Certainly, it could be that the computer doesn't turn on or that all network communication is down. These would be easy cases. As long as you have anything that looks or smells like a warranty in your agreement, you should be covered.

The problem arises because it's just never that simple. Typical IT problems are more like "the computers are too slow," "the network is too slow," "the system crashes too often," or "the website doesn't have some of the functionality we expected." Moreover, these are the types of problems that can lead to ugly disputes.

There is no magic after the problem arises. The solution is careful contracting at the front-end. For example, if you don't take the time to quantify the speed you expect from your network, where do you go with "it's too slow" when the other side says, "No, it is not too slow." If you lack an objective standard, you may just have a loser on your hands.

While there is no doubt that taking the time to carefully contract for IT services slows the date of the contract's signature, the only other choice would seem to be a wing and a prayer. Contracting, like any other process, simply takes time. Still, it can save your company if things go less than perfectly.

Using the custom development of a complex software product as an example, the norm in the IT industry is a vaguely worded warranty that says that the software will function according to its specifications, or some other vague document or attachment to your contract. The point is that the standard the software must meet is this "other document."

It's the norm because it's easy and provides at least some guidance. It's also often a poor way to go because this other document was not written to define your warranty and thus often doesn't have the objective standards against which you'll later want to judge your software.

Having said all this, have I ever had contracts where I've used some vague specifications as the benchmark for the warranty? I must confess that the answer is yes, I have.

The reasons are actually quite simple—it's all about time and money. Quite frequently, the parties don't want to take the time or spend the money necessary to prepare a more meaningful specifications document that was designed to serve as a benchmark for the warranty. We all know what a car should do. There's no similar common sense benchmark by which we can judge IT work. If you don't specify things in your contract, you may find yourself staring into the face of a bad situation.

IT contracting is often a time-consuming and resource-draining project. It takes effort to negotiate a deal and develop things like performance standards and acceptance testing procedures.

You could choose to march ahead with a contract that has as much definitive and clear material as a politician's stump speech. If all goes well, you'll feel like you made the correct judgment. However, in reality, you were just lucky. This method is okay for the desperate and those who like to play in the dark.

Who Takes the Loss?

When things go wrong in the world of IT, they can have far-reaching consequences. If your office network goes down, you have all the losses that go with the lack of productivity of your employees. If you're an airline and your reservation system crashes and burns, it's obvious how disastrous that could be. Who pays for these losses?

In IT, the answer is that the customer usually bears these risks. We can argue about how fair it is. The airline could say something like, "Let me get this straight. I pay you $5 million to update our reservation's software. It stops functioning, I lose millions of dollars, and you think that you shouldn't be responsible for that loss?"

The standard IT vendor's answer to the question is, "That's right!"

The vendor's perspective may not be obvious to many customers, but it does ring of legitimacy in many cases. As the customer, you must build mission-critical systems with enough redundancy and overcapacity to prevent catastrophic mishaps.

The argument would be that it was the fault of the airline in our scenario, which decided that running a parallel reservation's network or providing for more capacity was too expensive.

Similar arguments are made when other IT disasters happen. If you lose data, the vendor says that you should have had better backups. I could create other examples, but the point remains the same. It's up to the purchaser of IT services to create enough redundancy to protect against unacceptable losses.

The vendor's answer to legitimately broken or poorly performing IT products is we'll improve our "response time" in dealing with the issue, but we will never, ever, **ever**, write you a check for your losses. You must largely accept this fundamental norm.

Yes, there are exceptions. I have seen and negotiated contracts with real teeth against vendors, but they are the exceptions.

So, as a buyer of IT goods and services, focus on what you can get. You should always negotiate for better

response time guarantees than are first being offered. Follow this up by requesting specific escalation provisions, which helps to insure that if level one support can't get the job done in a reasonable amount of time, it will move up through the vendor's chain of command quickly. Good response time and escalation provisions can be worth their weight in gold when you're in crisis.

Some Red Flags—Damage Limitations

One of the things you should always focus on is damage limitations. Be leery of clauses like, "Vendor's liability for any loss, damage or expense of any kind, resulting from the products or services, negligence, or any other cause whatsoever, regardless of the form of action, whether in tort or in contract, shall be limited to the selling price of the products or services." Variations on this type of clause may limit you to six months of service charges or some predetermined, and usually low, dollar figure.

Limitations of liability are negotiable and since a one-sided damage limitation could emasculate much of what you gained in other aspects of your negotiation, I would suggest that you must focus on damage limits.

Here are some tips that can to some extent function as a partial checklist for you.

- Make the damage limitation mutual. What's good for the goose should be good for the gander. There is no justification for a limitation of liability that only benefits the vendor.
- Exclude third-party indemnity claims from the limitation. If a third party sues your company due to your vendor's misconduct, the limitation of liability should not limit your indemnity claim.
- Seek more than a refund as the damage limit. It just seems fundamentally unfair that the vendor has no skin in the game beyond a refund.
- Exclude willful repudiation of the contract from the damage limit. This is designed to prevent the vendor from repudiating your contract and damaging you because the vendor acquired a more lucrative customer. In that scenario, you really should be getting at least your expectation damages.
- Exclude breaches of the confidentiality provisions from the limitation of liability. I can just imagine a scenario where your confidential information is more valuable than the damage cap so they thoughtfully decide that theft of your information is profitable.

Final Tips from the Trenches

In negotiating your agreements, you must avoid that natural tendency to see the deal's starting point as being the vendor's form. You should first see the deal from your one-sided perspective. What do you want and need?

In a negotiation, you're not likely to get everything you want either, but you must work to pull contracts back to the middle, i.e., back to what's fair. You shouldn't ask for changes in a vendor's form only after asking yourself whether the change is significant. If it's one sided in favor of the vendor, ask that the provision be made neutral.

If the vendor asks that you indemnify them for your wrongdoing, you should ask that they indemnify you for their wrongdoing. If they get attorney's fees if they're the prevailing party, then you should if you're the prevailing party. If they can terminate the agreement if you sell your company, the reverse should be true.

After you've put every unfair provision on the table, you can use the issue of "significance" to decide which points to give up. Certainly, not every point has equal importance to you.

Just remember, what's good for them is good for you. That's fairness.

Don't walk into a deal thinking about how big they are. They want your business or they wouldn't be talking to you. Sure, the Microsofts of the world budge less than the local vendor down the road, but they all bend. The only way to find out how far is to push back.

Mark Grossman is a 26-year business lawyer who began focusing his practice on technology, telecom, and outsourcing deals about 20 years ago. Mark authored the book *Technology Law—What Every Business (and Business-Minded Person) Needs to Know*, and is a frequent speaker on technology law.

Not-For-Profit Governance Part II: Key Nonprofit Board Functions and Committees

by James A. Woehlke

This is the second in a series of articles on nonprofit governance. The first, "Nonprofit Governance: an Overview" was published in the Winter 2009 issue of *Inside*. This article addresses key board functions/committees for a nonprofit organization.[1] The next article will address the process of obtaining and maintaining tax exemptions.

Lawyers are often asked to join nonprofit boards to lend their legal acumen to the proper design, governance, and operation of the nonprofit. The instincts of a lawyer are important to these nonprofit activities, but the lawyer needs to maintain a broader perspective than merely meeting the requirements of the Secretary of State's Division of Corporations, Attorney General's Charities Bureau, Department of Taxation and Finance, and IRS. This broader perspective is required because she may be the only person on the board with a sense of the bad things that can happen to an organization if it becomes overly focused on its mission and neglects legal and regulatory obligations. This article sets out a governance framework to build good governance practices into an organization's culture.

As an organization grows, its board is likely to spin off committees responsible for each of the following functions, but even in the nascent nonprofit organization, these functions should be nurtured at the board level.

- Operations (Board committees include Executive and Staff Compensation.)
- Governance (Board committees include Audit for financial oversight and Governance for non-financial oversight, nominations and leadership development.)
- Finance (Board committees include Budget and Investment.)

Adhering to this framework will help assure that the IRS's "organized and operated" test is satisfied. That test, if met, assures that the organization will maintain its tax exemption over time. See, Treas. Reg. § 1.501(c)(3)-1. That being said, there is no fixed approach to committee structure. Some organizations create separate committees for each of the functions noted below; other organizations combine the functions to best suit their needs.

Operations Function/Executive Committee and Staff Compensation

N-PCL § 701(a) makes the board responsible for a nonprofit's management. Except for certain organizations benefiting youth, which may have one (and in limited circumstances more than one) board member as young as 16, a board member must be 18 years of age. An organization's board serves as its governing body. N-PCL § 701(b) authorizes the board to delegate management responsibilities to one or more non-board members and imposes on such non-board members the same liability for management incumbent on board members.

N-PCL § 717 describes the duties of directors and officers, setting the standard that board members discharge their duties in good faith and with the degree of diligence, care and skill which ordinarily prudent persons would exercise under similar circumstances. Board members, when acting in good faith, may rely on information, opinions, reports, or statements prepared by officers and employees believed to be reliable and outside experts to the extent the information is believed to be in their professional or expert competence. Also, a board can rely on duly constituted board committees as to matters within the authority granted to such committees by the certificate of incorporation, bylaws, or board resolution so long as that reliance is in good faith and within the prudent person standard. Section 717(b) closes with the following admonition and relief provision:

> Persons shall not be considered to be acting in good faith if they have knowledge concerning the matter in question that would cause such reliance to be unwarranted. Persons who so perform their duties [in accordance with the § 717 standard] shall have no liability by reason of being or having been directors or officers of the corporation.

Section 717 thereby codifies the business judgment rule. J. Seely, in *The Legal Guide for Association Board Members* (2010), at p. 78, elaborates on the business judgment rule as follows:

> To meet the standard of conduct, a board member is not responsible for conducting research of all pertinent information regarding any issue. Rather, the board member may rely on information provided by persons who the board member believes to be reliable and competent regarding the information presented. (Such persons could include officers and employees, legal counsel, accountants, and a committee of the board.) The reliance

must also be reasonable and the board member must make reasonable inquiry when it appears that reliance would not be appropriate under the circumstances. In summary, any board member, who is made aware of this legal standard of conduct, should have no trouble adhering her conduct to it.

Nevertheless, some nonprofit board members become complacent, perhaps relying on their experiences from other nonprofit boards that are less conscious of oversight responsibilities.

Executive Committee

Boards of directors meet periodically, often only quarterly or semi-annually. For an organization's governance to be on-going, larger boards often establish executive committees. N-PCL § 712 specifically authorizes nonprofit organizations to empower executive committees to act with full board authority except for the following actions:

(1) Submission to members of any action requiring members' approval under the N-PCL.

(2) Filling of vacancies in the board of directors or in any committee.

(3) Fixing of compensation of the directors for serving on the board or on any committee.

(4) Amendment or repeal of the bylaws or the adoption of new bylaws.

(5) Amendment or repeal of any resolution of the board which by its terms shall not be so amendable or repealable.

In addition, the organization's bylaws, standing rules established by the board, or the board resolution creating the executive committee may impose additional restrictions.

Often the executive committee is comprised of the organization's officers. However, other models are also used, such as including board members who can reflect different stakeholder segments. Another model includes officers and key board committee chairs. If an organization has a paid executive director, he or she is typically included on the executive committee, often as a nonvoting member.

A common concern with the use of executive committees is that they foster a perception among board members that the organization is being run by insiders and board members not serving on the executive committee are somehow second class. Another concern is that the board can begin to over-rely on the executive committee, leaving the full board merely to hear reports. This can cause a board's deliberative and decision-making skills to atrophy. Board members themselves can address these concerns with board actions limiting the authority of the executive committee or requiring greater transparency. Also, an executive committee can itself lessen these concerns by showing some restraint in the actions it takes. If a decision can wait till the next board meeting, for instance, the executive committee can make sure any necessary legwork is done, and then refer the matter to the board for final decision. Another approach to avoid a sense of "insider" domination is for executive committee members to consult other board members on executive committee matters, so long as the organization's confidentiality is preserved.

Staff Compensation Committee

A major exposure to nonprofit organizations exempt from tax under Internal Revenue Code [IRC] § 501(c)(3) is intermediate sanctions imposed by the IRS on compensation that exceeds guidance set out in Treasury regulations. Intermediate sanctions will be covered in another article in this series; but in brief, unreasonably high nonprofit executive compensation is considered an excess benefit that can result in severe penalties being imposed on the recipient, the organization, and those setting the unreasonably high compensation. See, IRC § 4958.

An important defense against the imposition of intermediate sanctions is the chartering of a staff compensation committee. The better practice, one observed by public, for-profit corporations, is to populate these committees solely with independent board members. In smaller organizations, the board or executive committee can undertake the task of setting staff compensation, but have any interested directors recuse themselves. Larger organizations engage expert compensation analysts, such as Hay Group (www.haygroup.com) or large CPA firms (though it is better not to use the same firm that audits the nonprofit) to assist their compensation committees. Others rely on survey resources from organizations such as the Economic Research Institute (www.eri-nonprofit-salaries.com) and the American Society of Association Executives (www.asaecenter.org). Still others conduct their own review of compensation reported on the annual IRS filings of organizations considered to be comparable, which are available gratis from Guidestar (www.guidestar.org). An organization that conducts its own research and analysis should be certain to document what organizations it considered comparable and why, and concrete reasons used to distinguish the salaries set by those organizations from those set by their committee or board.

Governance Function: Audit Committee

The audit function, which in larger nonprofits evolves into an audit committee, gives the board comfort that financial controls are appropriate to the organization and

operating well. The committee should be comprised of outside board members and ideally should not contain members of the organization's finance committee. In smaller organizations, interested board members should recuse themselves from much of the audit function deliberations. The board members charged with audit responsibilities need to perform several functions:

- Engaging the outside auditors and clarifying lines of authority: the auditor is to report not to staff, but to the audit committee and board;
- approving all services provided by the auditors;
- reviewing all auditor reports and discussing all significant issues identified by the auditors;
- monitoring to make sure the auditor's recommendations agreed to by the board are acted upon.

A comprehensive charter for an audit committee of a nonprofit professional society is available at http://www.nysscpa.org/governance/manual/audit_charter.htm. It is incumbent on board members charged with audit responsibilities to make sure the independent audit is meaningful. This means they should be wary of accepting the lowest bid from competing auditing firms. Some audits, although still within the parameters of professional standards, can be cursory. A "low ball" audit fee often should be a danger signal to the board. Before accepting such a proposal, the board should grill the "low ball" audit firm and its competitors about exactly why the fee is so low. Perhaps the "low ball" firm will test 10 transactions where a more thorough firm might test 50. Perhaps there is extra oversight by more senior auditors in the expensive audit. The audit committee should know what the organization might be missing out on.

The board should hold not just the staff, but also the auditors to the fire for the sake of the organization. For instance, when a board approves a budget, it is, for all intents and purposes, a policy decision that the board expects staff to follow. Frequently, auditors regard an organization's budget as an internal accounting document, not to be analyzed in the audit. If the board wants the auditor to test the extent to which staff is deviating from the budget without board approval, it needs to communicate that expectation to the auditor. Also, at the end of an audit, the CPA firm presents the nonprofit board a "management letter" identifying issues and making suggestions to improve the entity's financial function. Understandably, staff is nervous about management letters and the tendency for some board members to view any management letter suggestions as an indictment of the staff rather than as an opportunity for improvement. Given the wrong emphasis, staffs negotiate behind the scenes to neutralize the impact of management letters. This can cause an opportunity for improvement to be missed. The board should not only encourage, it should expect independent auditors to make meaningful suggestions for improvement. These suggestions often are the most valuable part of an auditor's services.

Board members who serve on an audit committee should do a little homework. A search of the Internet yields sample questions an audit committee should consider asking the auditor. See, for example: http://www.raffa.com/assets/File/audit_questions_after_planning_meeting.pdf and www.pwc.com/en_US/us/corporate-governance/assets/2010-shareholder-questions.pdf. Both of these resources are geared to for-profit enterprises. Additional areas of concern to nonprofit audit committees that could result in additional questions include the following:

- Is management adhering to the budget approved by the board? Are deviations from the budget receiving proper board approval?
- Is the organization staying true to mission? Is there evidence of mission drift?
- Is overhead being properly contained?
- Have any issues been noted that could result in problems on IRS examination?

Governance Committees

Governance committees are less common than audit committees, but equally important. They are responsible for making sure policies are in place to ensure proper behavior, not only of staff, but of the board itself, other volunteers, and the constituencies served by the organization. Important projects for governance committees include

- A code of ethics for board, volunteers, and staff. This needs to include procedures for enforcement. Examples of both a board code of conduct and enforcement policy are available at http://www.nysscpa.org/governance/manual/lp1.htm and http://www.nysscpa.org/governance/manual/lp2.htm. Also Robert's *Rules of Order* includes guidance on disciplining board members.
- A conflict of interest policy. A good concise conflict of interest policy is included in the Venable LLP article at http://www.venable.com/03-30-2005/.
- Procedures to ensure that the organization is complying with all tax and legal requirements.
- Standing rules for boards and executive committees. These are formalized procedures to encourage consistency in the way an organization is governed. They will vary from organization to organization. By way of example, standing rules adopted by the New York State Society of CPAs are available at

http://www.nysscpa.org/page/nysscpa-board-directors-standing-rules.

- Occasional bylaw revisions

In some organizations, the governance committee also serves the function of identifying future board candidates. In other organizations, separate nominating committees and leadership development committees are used for this purpose. Whichever approach is used, it is important that committees responsible for future board composition not be dominated by long-time board members or officers so as to avoid a board's becoming inbred or complacent.

Finance: Budget and Investment Committees

Part of a board's leadership development should be the recruitment of some business-savvy members who can focus on the financial side of the nonprofit. These individuals will be important in the development with staff of a meaningful budget for the organization and in the investment of its funds. Once the budget is developed and receives board approval, board members responsible for the financial budget function also police the degree to which staff is adhering to the budget, encourage transparency between staff and board regarding significant variances from budget, and recommend. In larger organizations these functions are divided into two separate committees. While it can occur that members of finance and investment committees also serve on audit committees, the better practice is to avoid overlap because their work may come into question by the auditor.

The next article in this series will discuss obtaining and maintaining of a nonprofit's tax exemption.

Endnote

1. Nonprofit organizations in this series include both public-benefit entities (such as social benefit organizations, colleges and universities, and nonprofit hospitals) and member-benefit entities (such as credit unions, trade associations, social clubs, and unions). To avoid confusion the person with the authority to preside over the board of directors, the chief volunteer officer, is referred to as the "chairperson" and the staff person with day-to-day management authority, the chief staff officer, is referred to as the "executive director."

James A. Woehlke is the General Counsel / COO of MBL Benefits Consulting Corp. Previously he served as General Counsel of the NYSSCPA and twice chaired the ACC Nonprofit Organizations Committee.

NYSBA Corporate Counsel Section
Kenneth G. Standard Diversity Internship Program
for Summer 2010
Kicks Off the 5th Year of Its Program

The Section has ten interns this summer working with in house counsel offices.

FINRA (Financial Industry Regulatory Authority, Inc.), Pfizer, Pepsi, Alliance Bernstein and the New York Power Authority (NYPA) are hosting students this year from Albany Law School, Brooklyn Law School, Hofstra School of Law, New York Law School, Pace School of Law, and St. John's University School of Law.

We have placed fourteen other interns over the past four years.

Past in house counsel offices have included FINRA, Goldman Sachs, Con Edison, McGraw-Hill, Oneida, Pfizer and the Institute for Conflict Prevention & Resolution.

Past law schools which have participated in the Program have included many of those listed above, as well as Buffalo Law School, Cardoza School of Law and CUNY School of Law. We have also solicited students from Columbia Law School, Fordham University School of Law and NYU School of Law. It is our intention to work with Cornell Law School, Syracuse University College of Law, and Touro College Law Center in future years.

We typically fully sponsor one student at a not-for-profit by giving the host organization the student's full salary for the summer. Otherwise, we generally contribute half of the student's salary for summer and the host companies contribute the other half. However, many of our host companies fully provide for the student's salary for the summer. Due to the generosity of many host companies, more students each year are able to participate in the program.

We also host annually an event honoring current and past interns, host companies, law schools and Ken Standard to name a few.

We would like to thank the Section members of the NYSBA Corporate Counsel Section for their sponsorship of this program.

Those interested in participating as a host company are encourage to contact Jean E. Nelson of the New York State Bar at jnelson@nysba.org or 518-487-5588.

From the NYSBA Book Store >

Counseling Content Providers in the Digital Age

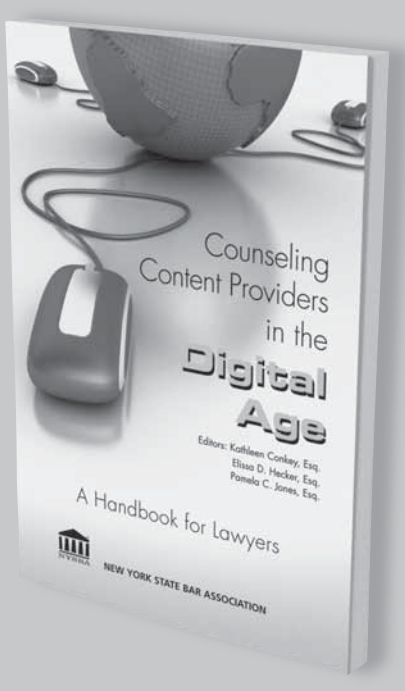
A Handbook for Lawyers

For as long as there have been printing presses, there have been accusations of libel, invasion of privacy, intellectual property infringements and a variety of other torts. Now that much of the content reaching the public is distributed over the Internet, television (including cable and satellite), radio and film as well as in print, the field of pre-publication review has become more complicated and more important. *Counseling Content Providers in the Digital Age* provides an overview of the issues content reviewers face repeatedly.

Counseling Content Providers in the Digital Age was written and edited by experienced media law attorneys from California and New York. This book is invaluable to attorneys entering the field of pre-publication review as well as anyone responsible for vetting the content of their client's or their firm's Web site.

Table of Contents
Introduction; Defamation; The Invasion of Privacy Torts; Right of Publicity; Other News-gathering Torts; Copyright Infringement; Trademark Infringement; Rights and Clearances; Errors and Omissions Insurance; Contracting with Minors; Television Standards and Practices; Reality Television Pranks and Sensitive Subject Matter; Miscellaneous Steps in Pre-Broadcast Review.

NEW!



EDITORS
Kathleen Conkey, Esq.
Elissa D. Hecker, Esq.
Pamela C. Jones, Esq.

PRODUCT INFO AND PRICES
2010 / approx. 430 pages, softbound / PN: 4063

$50 NYSBA Members
$65 Nonmembers

$5.95 shipping and handling within the continental U.S. The cost for shipping and handling outside the continental U.S. will be based on destination and added to your order. Prices do not include applicable sales tax.

Get the Information Edge

1.800.582.2452 www.nysba.org/pubs

Mention Code: PUB0829N

NYSBA

Corporate Counsel Section Committee Chairpersons

CLE and Meetings
Steven G. Nachimson
Compass Group USA, Inc.
3 International Drive, 2nd Floor
Rye Brook, NY 10573

Howard S. Shafer
Shafer Glazer LLP
90 John Street, Suite 701
New York, NY 10038-3202
hshafer@shaferglazer.com

Diversity Internship
David S. Rothenberg
Goldman Sachs
200 West Street, 40th Floor
New York, NY 10282
david.rothenberg@gs.com

INSIDE/ Publications
Janice Handler
handlerj@aol.com

Allison B. Tomlinson
Gensler
1230 Avenue of the Americas
Suite 1500
New York, NY 10020
allison_tomlinson@gensler.com

Membership
Thomas A. Reed
1172 Park Avenue
New York, NY 10128
tomreed2@me.com

Pro Bono
Steven H. Mosenson
The Center for Discovery
P.O. Box 840
Harris, NY 12742
smosenson@sdtc.org

Technology and New Media
Fawn M. Horvath
Senior Counsel
Macy's, Inc.
11 Penn Plaza, 11th Floor
New York, NY 10001

Julie Ko
julieko@gmail.com

NEW YORK STATE BAR ASSOCIATION
CORPORATE COUNSEL SECTION
One Elk Street, Albany, New York 12207-1002

ADDRESS SERVICE REQUESTED

NON PROFIT ORG.
U.S. POSTAGE
PAID
ALBANY, N.Y.
PERMIT NO. 155

Inside is a publication of the Corporate Counsel Section of the New York State Bar Association. Members of the Section receive a subscription to the publication without charge. Each article in this publication represents the author's viewpoint and not that of the Editors, Section Officers or Section. The accuracy of the sources used and the cases, statutes, rules, legislation and other references cited is the responsibility of the respective authors.

ISSN 0736-0150 (print) 1933-8597 (online)

Inside

Section Officers

Chairperson
Allison B. Tomlinson
Gensler
1230 Avenue of the Americas, Suite 1500
New York, NY 10020
allison_tomlinson@gensler.com

Chairperson-Elect
Gregory H. Hoffman
North American Livecareer
745 Fifth Avenue, Suite 902
New York, NY 10151
greg@livecareer.com

Vice-Chairperson
Howard S. Shafer
Shafer Glazer LLP
90 John Street, Suite 701
New York, NY 10038-3202
hshafer@shaferglazer.com

Secretary
Sarah M. Feingold
Etsy Inc.
55 Washington Street, Suite 512
Brooklyn, NY 11201
sarahfeingold@gmail.com

Treasurer and Vice-Chairperson
David S. Rothenberg
Goldman Sachs
200 West Street, 40th Floor
New York, NY 10282
david.rothenberg@gs.com