

Inside

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

Message from the Chair



To the Members of the Corporate Counsel Section:

You will be reading this message from me—my final one as your 2014 Chair—around the time of the Annual Meeting of the New York State Bar Association and the Corporate Counsel Section in January 2015. I'm happy to report that the state of our Section remains very healthy,

and we have been active on a number of fronts over the course of the year.

KGS Diversity Internship Program and Reception

My last message anticipated the annual reception that was sponsored by the Corporate Counsel Section on July 23, 2014 to honor the law student interns and their employers who participated in this year's Kenneth G. Standard Diversity Internship Program. Since I wrote about it in detail then, and there is a separate article in this issue concerning the reception by *Inside* Co-Editor Matthew Bobrow, let me just add that we continue to be enormously grateful to Executive Committee member Anne Atkinson and her firm, Pryor Cashman LLP, for hosting this event in their beautiful Times Square offices; to Executive Committee member Dave Rothenberg and his Committee on Diversity, for all their many hours of hard work in organizing and running this program so successfully year after year; to this year's host

Inside

Inside <i>Inside</i>3 (Jessica Thaler and Matthew Bobrow)	Being Prepared When the Cloud Rolls In.....18 (Natalie Sulimani)
Security Concerns for Law Firms: Strategies and Best Practices for Building Security 4 (Gary B. Fiebert)	Cybersecurity Due Diligence in Corporate Acquisitions.....21 (Joseph V. DeMarco and Jeremy Apple)
Workplace Violence—An Employer's Duty to Protect Employees from Harm..... 7 (Howard S. Shafer)	How to Slay the Cyber Dragon: Lawyer-Supervised Privacy Programs.....24 (Bruce H. Raymond)
Weapons in the Workplace—Rights and Risks..... 9 (Brian T. Stapleton)	Social Media Evidence: To Authenticate or Not to Authenticate?28 (Adam Cohen)
Report on the Kenneth G. Standard Diversity Reception..... 11 (Matt Bobrow)	Use and Defense of Data Subpoenas.....30 (Charles Ross and Anne van Greevenbroek)
The Boneyard..... 13 (Robert Cioffi)	Damned if You Don't: Addressing Law Firm E-Discovery and Data Security Challenges.....33 (John J. Jablonski)
Protecting Proprietary and Other Information When Using Third Party Vendors 15 (Kenneth C. Citarella)	

companies and organizations, namely The Visiting Nurse Service of New York, The ACE Group, AllianceBernstein, NYSTEC, Pepsi Co., Inc., Pitney Bowes Inc., and Salesforce.com, for providing this wonderful opportunity to the interns; to the many New York State Bar Association leaders and New York State judges who underlined the importance of this program by honoring us with their presence at the reception; to the Kaplan Bar Review, for co-sponsoring the event and underwriting generous prizes for the interns; and finally, to the wonderful class of 2014 interns themselves, all of whom shared with us how much this opportunity meant to them individually, and who we hope will go on to become active members of and contributors to the New York State Bar Association through the Corporate Counsel Section or otherwise.

Ethics for Corporate Counsel 2014 and Other CLE Programs

Our Section's very well regarded Ethics for Corporate Counsel CLE program, once again under the auspices of Program Chair, Steve Nachimson (Compass Group USA, Inc.), and Panel Chair, Michael S. Ross (Law Offices of Michael S. Ross), was offered this year on the afternoon of Thursday, October 23, 2014 from 1:00–4:30 pm at the Cornell Club in Manhattan. Program topics included privilege issues, conflicts, supervision of in-house staff, etc., and also focused on the rule of corporate counsel in regulatory investigations. In addition to Mr. Ross, the panel consisted of Mark S. Cohen (Cohen & Gresser LLP); Anthony E. Davis (Hinshaw & Culbertson, LLP); Naomi F. Goldstein (Departmental Disciplinary Committee, NYS Supreme Court, First Department); and Jerome G. Snider (Davis, Polk & Wardwell). The program was followed by an hour-long Member Appreciation and Networking reception (free to Section members).

On November 20, 2014, our Section co-sponsored with the Law Practice Management Committee (chaired by our Executive Committee member and *Inside* Co-editor, Jessica Thaler) a full day, 7 credit hour CLE summit in Manhattan on "Hot Topics in Law Practice Management," specifically addressing security concerns. Various expert speakers and panels covered Office and Physical Security, Technology in the Workplace and Equipment Security, Metadata, and eDiscovery and Litigation/Security concerns. Registration for this valuable and highly relevant program cost only \$125 for Section members. I hope a good number of you were able to attend, but if you missed it, just continue to read the balance of this issue of *Inside*, much of which is devoted to written submissions by the panelists who presented this program.

Corporate Counsel Section Web Page and "Community"

I have explained in prior Messages that the New York State Bar Association is slowly but steadily introducing electronic "communities" as an adjunct to the

nysba.org website. Members of the Section's Executive Committee have been using our own private Community for several months now as a common repository for Section-related documents such as minutes of meetings and event rosters, announcements and notices, and discussions on topics of common interest. We are now preparing to open up the larger Corporate Counsel Section-wide community, which will be available to all Section members in addition to the Executive Committee. I strongly encourage you to join this new Community as soon as you receive your email notification of its availability. This email will include complete instructions as to what you need to do to join.

As with all NYSBA communities, each Community member can select how to receive email communications from the Community, whether in real time, or via a daily or weekly digest. We have found that participation in our EC Community has been slowly but steadily increasing. There are a number of other Communities on the nysba.org website that are already accessible to all NYSBA members, such as the Technology Community. The more Section members who join and become active by starting discussions on any topic you think might possibly of interest to others in the Community, or who ask questions to which others in the Community may respond, the more valuable a resource it will be to the Section as a whole. My hope is that in due course, but sooner rather than later, the Section Community will become a valuable "commons" from which all Section members can draw some benefit. Just how great the benefit will be will depend on each and every one of our Section members who decide to contribute to it.

Member Appreciation and Networking and Other Events

Our second 2014 MA&N event took place on October 23, 2014 at The Cornell Club in Manhattan, immediately following the Ethics for Corporate Counsel CLE program described above. Over 90 people attended this event, and I feel certain that those who did come found it both fun and worthwhile. Another MA&N event has been scheduled for June 18, 2015, once again at Upstairs at the Kimberly in Manhattan. Further details and an invitation to register will be forthcoming closer to the event.

Annual Meeting of the Section and Two January CLE Programs

The Annual Meeting of the Corporate Counsel Section will be held on Wednesday, January 28, 2015 at the New York Hilton Midtown in Manhattan, beginning at 8:30 a.m., to elect officers and EC members for 2015. As of this writing, I can definitely say that our Section this year is co-sponsoring not just one, but two CLE programs that week. The first one, in conjunction with the Business Law Section, will take place on January 28th immediately fol-

(continued on page 3)

Inside Inside

We are excited to bring you our first *Inside* issue as co-editors. The theme of this edition of *Inside* is “security” and addresses a broad range of issues such as protecting your office and employees, safeguarding your equipment and network, shielding cyber and other information, and defending and exploiting the use of information, including metadata, in litigation through e-discovery and data subpoenas. This edition is a follow-up to a joint program held in New York City by the Corporate Counsel Section and the Law Practice Management Committee in November 2014. We want to extend a special thank you to the panelists from that program, especially those who are also contributors to this issue of *Inside*.

We have also included a report on the Kenneth G. Standard Diversity Reception honoring the interns and host sponsors who participated in the Corporate Counsel Section’s Kenneth G. Standard Internship Program in 2014, the program’s 9th year. Since its inception in 2006, the program has matched 54 interns and host sponsors.

We are looking for contributions for our upcoming issues of *Inside*. If you would like to publish, please contact us directly. Our contact information appears on p. 32 in this newsletter. We look forward to working with many of *Inside*’s past and future contributors to provide Section members with articles of interest and relevance to their practices.

Jessica Thaler and Matthew Bobrow

Jessica Thaler is an attorney with Bliss Lawyers, currently working on secondment for Credit Suisse. Prior to engaging with Bliss, she spent a year acting as the Chief Legal Officer of My Sisters’ Place, a not-for-profit organization working for the benefit of domestic violence and human trafficking victims throughout Westchester County. Jessica has a rich experience as a corporate-transactional generalist, gained through her work at NYC law firms and her solo practice. She is an active member of NYSBA, acting as immediate past chair of the Committee on Lawyers in Transition, on the executive committees for EASL and Corporate Counsel Sections, as a long-standing member of the Membership Committee and the Committee on Law Practice Management and, now, as a co-editor of *Inside*. Jessica is also a House of Delegates representative for the Westchester County Bar Association. She is a graduate of UCLA, cum laude (1995), and Fordham University School of Law (1999).

Matthew Bobrow is a 3L law student at New York Law School where he is a Staff Editor for the *New York Law School Law Review*. He is participating in a training program with a Legal and Compliance rotations at Credit Suisse AG and is law clerking with Shafer Glazer LLP. Matthew is excited to be helping edit his first issue of *Inside*. Whenever possible, he is always looking for ways to contribute to the New York City legal community.

Message from the Chair

(Continued from page 2)

lowing the Annual Meeting of the Section. We are doing the second program, a full-day CLE, in conjunction with the Dispute Resolution Section, on Thursday, January 29th, starting at 9:00 am. Detailed topics and speakers for each of these programs are still being worked out at this writing, but I believe you will have received full details and an opportunity to register for each of these programs well before you see these words in print.

New Editors for *Inside*

This issue of *Inside* is the first to be co-edited by our new editorial team of Executive Committee member Jessica Thaler and law student Corporate Counsel Section member Matthew Bobrow. Please join me in welcoming Jessica and Matt, in thanking them for their hard work in putting together their inaugural issue, and in giving them any feedback you have concerning our Section’s flagship

publication, either with respect to this issue or for future issues.

Goodbye but Not Farewell

My second term as Chair of this Section ends more or less simultaneously with the appearance of this issue of *Inside*. Although I will no longer be your Chair, it is my hope and expectation to continue to take an active part in helping to manage the affairs of the Section in my capacity as Immediate Past Chair for the coming year, and after that to remain a member of the Section’s Executive Committee for as long as the Section sees fit to continue me in that role. It has been a genuine pleasure to serve the Section as whole as well as many of you individually during this time, and I greatly look forward to continuing to do so.

Tom Reed

Security Concerns for Law Firms: Strategies and Best Practices for Building Security

By Gary B. Fiebert

Introduction

We live in interesting and challenging times. Not a day goes by when we do not hear at least one news report, from somewhere around the country, as well as from cities across the globe, describing an event that impacted the safety and security of people—innocent bystanders, military and law enforcement personnel, commercial and residential properties. As a result of the globalization of the broadcast media and the explosion of social media networks, we learn and see these events unfolding before our eyes. And while many people still believe that *“accidents only happen to others,”* this daily diet of *“bad news”* has heightened our awareness and concerns for the safety and security of each of us and our loved ones.

It is no wonder, then, that office and building security has become a key concern of all.

First Priority: Personnel

Employees (from the junior-most staff positions up the organization chart through senior management as well as the partners) must each feel safe, secure and important in the workplace. This is a fundamental truth. In fact, employees who do not feel safe, secure and important *will not* participate in, or be motivated to, protect and secure the premises, your equipment or important records and documents. Creating and maintaining an environment where the safety, security and importance of all is recognized by all personnel as a key responsibility of management.

Relying on news reports and social media broadcasts is not enough to build awareness in the workplace. Periodic and regular internal communications about safety and security are required to foster a mindset of *“if you see something, say something.”* Personnel at every level need training and education on safety and security issues. Conduct drills on a regular basis for all personnel. In addition to the *“fire safety teams”* that many office buildings require of their tenants, your firm may provide CPR training, other onsite first aid procedures and physical layouts that limit access to various parts of your premises, and a host of other policies and procedures that establish a sense of safety and security among your personnel.

New employees require orientation into the safety procedures of your firm. And all personnel must be aware of their roles and responsibilities during the many different types of events that can occur and negatively impact the safety and security of all. This is especially

important in order to convey the sense that your management has prepared the firm to anticipate and mitigate the possibility of an event occurring, along with the necessity to be ready if an emergency event occurs rather than just being in a position to react to such an event if and when it occurs.

Prepare and Implement a Safety and Security Plan

All of these management responsibilities for a safe and secure workplace environment presuppose that you have developed and implemented a safety and security plan for your workplace. Several firms I am familiar with have these plans created and updated by members of their Business Continuity Committees. Other firms have tasked their Risk Management Committee with the planning responsibility. And still other firms look to their facilities management team for the plan. Whichever approach you select, it is useful to involve representatives from other parts of the firm, beyond facilities management, including human resources, finance and accounting, information technology, case management and others depending upon your firm's practice profile.

As part of your safety and security planning process, it will be important to evaluate and document the current way of doing things—things like controlling access to the building and your premises, means of communicating with your personnel during and immediately after an *“event,”* and coordination with building personnel.

The result of this plan should include an update to your existing policies and procedures for safety and security. It should also include a series of both near- and longer-term goals for enhancing safety and security.

Some examples of near-term goals might include the addition of locks to access doors; setting parameters for after-hours access to your premises; establishing codes and other improvements for your internal communications and establishing protocols for visitor and vendor access to your premises.

For the longer term, you should set a regular and periodic schedule for meeting with building management to review and discuss security issues; review your internal *“security”* staffing levels, roles and responsibilities, physically alter your space and establish physical stores of emergency supplies, *“fanny packs,”* and protocols to replenish and refresh them.

Having a plan in place, supported by policies, procedures and protocols, however, is not enough to ensure that you are creating and maintaining a safe and secure

workplace environment. Develop the habit of constantly and continuously reviewing the plan and the results of your drills. Ask what can be done differently to make things more secure? Make note of the things that are being done correctly and compliment and thank those staffers involved for their efforts and attention. Routinely consider what, if any, additional resources are required.

Security Breaching Events

After the tragic events of September 11, 2001, I recall discussions with some members of the Executive Committee, at the firm where I was then Executive Director, regarding the steps we needed to take to become a safer and more secure workplace. But a few senior partners felt that the 9/11 events were such a unique occurrence that they were not likely to recur. As such, they were not enamored with increasing our spending for safety and security. Fortunately, I convinced the majority of the committee and we increased our preparedness and readiness. Over the ensuing years, many of the types of events outlined below occurred and we were ready for each of them.

The most frequent safety and security event involves unauthorized access to your premises. The results of such access may be burglary, robbery, acts of violence against targeted or random personnel, acts of terrorism, or even industrial/corporate espionage.

There are also external acts that can have a direct, negative impact upon your premises and your personnel. These acts include letter/package bombs, car bombs, chemicals, hazardous odors and radiation.

All of these aforementioned events involve one or more perpetrators who are intent upon negatively impacting the safety and security of your premises and personnel. But a well-conceived safety and security plan must also consider an array of events that can result in limited (or loss of) access to your premises as well as injuries to personnel. And such events may not even occur on or in your premises, but could impact you even if they are in the next building, next block or across town. The most obvious of these events are fires and floods. Sometimes these are caused by building issues and sometimes these events have nothing to do with your building directly. There are other building infrastructure events including electrical or utility outages, structural deficiencies, and other service outages. And, of course, there are always weather-related events.

Each type of event needs to be considered and addressed in your plan for each one creates unique opportunities to ensure your workplace remains safe and secure.

Subsequent Priorities

Since the most frequent safety and security breach involves access to your premises, I cannot emphasize enough the importance of ensuring that you have addressed all of the issues.

There are several categories of visitors (and intruders) who may attempt to gain access to your premises and the steps you and building management take to secure access need to consider these different types of visitors.

Beyond employees, there are former employees. Do your employees need photo identification or electronic card access to enter the building? Are such IDs/card and door keys taken from former employees upon termination? Do you notify building security whenever an employee terminates so as to restrict future access?

Outside visitors will include soliciting sales people and other uninvited guests; invited visitors including clients, adversaries, and others, as well as vendors and trades people and various and sundry contractors.

Any and all of these categories may seek access during normal work hours or off-hours including nights and weekends. Each door to the building, along with each door to your premises, must address the access issue. This can be exacerbated if your building also has indoor parking with direct access to your premises from the garage.

The next greatest cause of security or safety breach involves mail and package delivery. In addition to the procedures and protocols associated with daily mail delivery service, your plan should consider the movement of parcels in and out of your premises. And you need exception routines to accommodate special deliveries, process service, deliveries of supplies, transfer of files and other similar “exceptions.”

Anticipate Recovery Requirements

Because my crystal ball is not any better than anyone else’s crystal ball, I still have not come up with a way to definitively lay out a recovery plan absent the details of the event we are trying to recover from. But you can make some assumptions and build a portion of your plan for a recovery from any of the aforementioned events, based upon a reasonable set of assumptions. This additional planning, combined with some desktop tests and drills, will further help your preparedness.

And there are still other steps you can consider taking. For example, in my experience as an Executive Director/COO for three large NYC-based firms over a twenty year period, I can recall a few events where we lost access to our premises and the Executive Committee asked me to arrange an off-site meeting place for us for a few days while we assessed the damages to the firm and the steps we would need to take to get back to “business as usual.” Having lived through arranging meeting rooms at a hotel or meeting in the home of one or another member of management, I started the New York City Law Firm Command Center Compact. Together with the Executive Directors/COOs of about two dozen other larger NYC law firms, we created a compact where each firm was “paired” with two other firms—one in their immediate vi-

Workplace Violence—An Employer’s Duty to Protect Employees from Harm

By Howard S. Shafer

Introduction

Approximately 2 million employees are victims of workplace violence each year.¹ Employees are exposed to violence ranging from violent actions of third parties or co-workers to harmful threats from spouses. Workplace violence is an issue that not only affects the safety of the employee, but also touches on employers’ liability to their employees. Moreover, recent shootings and stabbings have opened up a debate on the duty owed by an employer to protect an employee.

On September 26, 2014, Alton Nolen, a former employee of Vaughn Foods, was suspended from his job for unknown reasons.² Following his suspension, Nolen went home to retrieve a knife and returned to his workplace to injure his co-workers.³ Nolen beheaded one co-worker and violently stabbed another co-worker.⁴ Officials remain unaware as to the reason behind these attacks. In order to address this type of issue, New York has implemented workers’ compensation laws and asserted a common law duty for employers to protect against employees who deliberately harm others.⁵

Employer’s Duty

At common law, employers owe no duty to protect employees from harm in the workplace. New York state laws and federal regulations do require standards for safe work environments. For example, New York Labor Law Section 200 mandates that persons employed in the workplace be provided with a safe place to work.⁶ OSHA provides similar protections.

With no common law or statutory framework to impose a duty, workplace violence and an employer’s duty is an area of the law which is developing.

In New York, courts have held that an employer can assume a duty to protect an employee from harm where one does not exist. In *Ruiz v. Griffin*,⁷ plaintiff brought a wrongful death suit against her husband’s employer for negligently protecting her husband. Timothy Ruiz, plaintiff’s decedent, was an employee of defendant Old Navy. During the course of his employment, he received anonymous threats and acts of vandalism against his car. As a result, Old Navy employed loss prevention agents to escort him from the store to his car. Defendant Griffin was jealous of Ruiz’s friendship with a coworker and fatally shot Ruiz as he was walking to his car. Ruiz’s loss prevention agents had stopped to retrieve a cigarette and Ruiz was unaccompanied at the time of the shooting. Plaintiff submitted evidence to raise triable issues of fact as to whether Old Navy knew or should have known of a

likelihood that a third person might endanger her husband’s safety. Plaintiff also raised an issue as to whether Old Navy satisfied the duty, if there was a duty, to offer protection against criminal activity.

This case did not impose liability on the employer. Instead, the court granted the plaintiff leave to amend the claims to assert causes of action which could give rise to the employer’s liability. It should be noted that the motion to amend the claims was unopposed.

Violence in the Workplace—A Statutory Framework For Public Employers

In response to the rising number of violent workplace crimes, New York, like many other states, has enacted legislation to address workplace violence through the Workplace Violence Prevention Act (WVPA).⁸ Rules have also been promulgated by the Commissioner of the New York State Department of Labor to address the issue.⁹

The WVPA applies to public employers with more than 20 employees. In broad terms it requires a risk evaluation and determination; a written violence protection program; employee information and training; and a notice procedure for the reporting of imminent dangers or threats.

Pursuant to the authority granted in the statute, the Commissioner did implement rules, codified at 12 NYCRR §800.6, but only applicable public employers.

Neither the statute nor the rules spell out the consequences to the public employer for failure to comply. However, it does grant the Commissioner would have the authority to issue penalties as with any other Labor Law violation. Violation of any provision of the Labor Law, the Industrial Code, or any rule, regulation, or lawful order of the Department of Labor, is a misdemeanor and is punishable by fine or imprisonment, or both. The Labor Law also provides for the imposition of civil penalties for each violation of labor law governing the employment of minors under 18 years of age by an employer. The penalties are fines of up to \$1,000 for the first violation, \$2,000, for the second, and \$3,000 for the third and subsequent violations. The largest penalty for injury or death is triple the maximum penalty allowed under the law for such a violation.

It doesn’t end there. The Federal Fair Labor Standards Act authorizes the Secretary of Labor to assess a civil money penalty of up to \$10,000 for each violation of the labor provisions regarding minors or any of its regula-

tions. This penalty is in addition to those provisions for fines, imprisonment, or restraint by injunction.

Workers' Compensation and Violence in the Workplace

Generally, the New York Workers' Compensation Law as a whole affords damages to injured employees for acts occurring at the place of employment.¹⁰ Additionally, Section 11 of the New York Workers' Compensation Law serves to protect the interests of employers and injured workers in cases of workplace injury and violence by barring third-party actions against them except in extremely limited circumstances, and limits an employer's liability for an employee's on-the-job injury to workers' compensation benefits.¹¹

In *Wilson v. Danka Corp.*,¹² a co-employee sexually and physically assaulted plaintiff. This injury occurred when both individuals were on a work trip for their employer, Danka Corporation. Plaintiff alleged that defendant employer violated its duty to protect her safety during employment as well as failed to reprimand the assaulter for his attack on plaintiff. The court determined that an employer cannot be held for tortious acts committed by the employee for motives that are unrelated to the furtherance of the employer's business. The court also barred plaintiff's breach of duty claim by stating that workers' compensation is the exclusive remedy available to employees who are injured during the course of their employment. Since the injury occurred on a work trip, plaintiff was not allowed to bring a negligence claim against the employer. This case demonstrates the protection afforded to employers by the Workers' Compensation Laws.

Conclusion

Currently, only public employers in New York are subject to the WVPA. Nevertheless, even private employers can assume a duty to their employees where none exists based upon their conduct. Except in very limited circumstances, the New York State Workers' Compensation Law would protect an employer from a civil action

by a covered employee. The state of the law is, however, in flux. With the media attention to workplace violence and the existing statute covering public employers, similar obligations will likely be imposed upon private employers.

Endnotes

1. U.S. Dept. of Labor, Occupational Safety and Health Admin., *Workplace Violence*, OSHA Fact Sheet, OSHA (2002), available at https://www.osha.gov/OshDoc/data_General_Facts/factsheet-workplace-violence.pdf.
2. See Richard Perez-Pena & Michael S. Schmidt, *Woman Is Beheaded in Attack at Oklahoma Food Plant*, THE NEW YORK TIMES, Sept. 26, 2014, available at http://www.nytimes.com/2014/09/27/us/oklahoma-man-is-said-to-behead-co-worker.html?_r=1.
3. See Abby Ohlheiser, *What We Know About Alton Nolen, Who Has Been Charged with Murder in the Oklahoma Beheading Case*, THE WASHINGTON POST, Sept. 30, 2014, available at <http://www.washingtonpost.com/news/post-nation/wp/2014/09/30/what-we-know-about-alton-nolen-who-has-been-charged-with-murder-in-the-oklahoma-beheading-case/>.
4. Ohlheiser, *supra*.
5. New York State Elec. and Gas Corp v. Sys. Council U-7 of IBEW, 328 F. Supp.2d 313, 316 (N.D.N.Y. 2004).
6. N.Y. LAB. LAW § 200 (McKinney 1962).
7. Ruiz v. Griffin, 71 A.D.3d 1112 (N.Y. App. Div. 2d Dep't. 2010).
8. N.Y. LAB. LAW § 27-b (McKinney 1975).
9. 12 N.Y.C.R.R. Law § 800.6 (1970).
10. N.Y. WORKERS' COMP. LAW § 11 (Consol. 2009).
11. *Castro v. United Container Machinery Group, Inc.*, 96 N.Y.2d 398 (2001); *Fleming v. Graham*, 10 N.Y.3d 298, 300 (2008).
12. *Wilson v. Danka Co.*, 01 Civ. 10592 (DAB)(FM), 2002 U.S. Dist. LEXIS 25055 (S.D.N.Y. Dec 10, 2002).

Howard S. Shafer, Esq. is a Partner in the firm of Shafer Glazer, LLP, the Immediate Past Chair of the Corporate Counsel Section of the New York State Bar Association and President of Your House Counsel®. Shafer Glazer, LLP concentrates its practice in the areas of Insurance and Corporate Liability Defense and acts as Outside General Counsel to small and mid-size companies. Howard can be reached at HShafer@ShaferGlazer.com. Palak Patel, a Law Student at Brooklyn Law School, assisted in the preparation of this article.



CHECK US OUT ON THE WEB
<http://www.nysba.org/Corporate>

Weapons in the Workplace—Rights and Risks

By Brian T. Stapleton

I. Introduction and Summary

In *District of Columbia v. Heller*, 554 U.S. 570 (2008), the Supreme Court resolved a question that had been the subject of ongoing debate for the better part of a century. The Court concluded that the text, structure, and history of the Second Amendment “conferred an individual right to keep and bear arms.” *Id.* at 595. Two years later, the Court concluded in *McDonald v. City of Chicago*, 130 S. Ct. 3020, 3026 (2010), that this individual right is a fundamental one that applies with full force to the States.

Heller’s holding was contrary to the law that had governed most of the nation, including in the Second Circuit. See *Bach v. Pataki*, 408 F.3d 75, 83-6 (2d Cir. 2005). In the wake of these decisions one might have expected to see states and municipalities respond by examining their laws to determine whether they were consistent with the fundamental individual right the Supreme Court recognized. Instead, many states and municipalities have doubled down. This is particularly true in New York State and New York City, which have some of the most restrictive firearms laws and regulations in the United States.

Generally speaking, one cannot possess a handgun in one’s place of business anywhere in New York unless that possession is licensed. A license is not required to possess a long arm at a business place outside of New York City. Within New York City, all long arms must be licensed. Throughout the state, all “grandfathered” long arms that constitute “assault weapons” as defined by New York’s SAFE Act must be registered with the State Police. Provided this is done, the same can be possessed at one’s home or place of business. As long as possession is licensed, one has a right to possess a firearm at one’s place of business. Those who engage in unlicensed possession in the workplace risk loss of the firearm, criminal prosecution, and possible imprisonment.

II. New York State Licensing Regime

New York law requires an individual to obtain a permit in order to possess a firearm in his or her home or place of business. N.Y. PENAL LAW § 265.01 (Consol. 2013); § 265.20(a)(3); § 400.00.

The statewide requirements for obtaining a permit are governed by N.Y. PENAL LAW § 400.00 (Consol. 2013). Under § 400.00(1), no firearm shall be issued or renewed except for an applicant who:

- (a) is twenty-one years of age or older (unless honorably discharged from the United States army, navy, marine corps, air force or coast guard, or the national guard of the state of New York, in which case no such age restrictions apply);

- (b) is of good moral character;
- (c) has not been convicted anywhere of a felony or a serious offense;
- (d) is not a fugitive from justice;
- (e) is not an unlawful user of or addicted to any controlled substance;
- (f) if an alien (i) is not illegally or unlawfully in the United States or (ii) has not been admitted to the United States under a nonimmigrant visa subject to the exception in 18 U.S.C. § 922(y)(2);
- (g) has not been discharged from the Armed Forces under dishonorable conditions;
- (h) having been a citizen of the United States, has not renounced his or her citizenship;
- (i) has stated whether he or she has ever suffered any mental illness;
- (j) has not had a license revoked or who is not under a suspension or ineligibility order issued pursuant to the provisions of N.Y. CRIM. PROC. LAW § 530.14 (Consol. 2013) or N.Y. FAM. CT. ACT § 842(a) (Consol. 2013);
- (k) in Westchester County, has successfully completed a firearms safety course;
- (l) has not had a guardian appointed for him or her pursuant to any provision of state law, based on a determination that as a result of marked subnormal intelligence, mental illness, incapacity, condition or disease, he or she lacks the mental capacity to contract or manage his or her own affairs; and
- (n) presents no good cause for the denial of the license.

There are several different types of licenses that one can obtain under New York’s statutory scheme. Under N.Y. PENAL LAW § 400.00(2) (Consol. 2013), licenses include:

- (a) to engage in the business of gunsmith or dealer in firearms;
- (b) to have and possess in a dwelling by a householder;
- (c) to have and possess in his place of business by a merchant or storekeeper;

- (d) to have and carry concealed while so employed by a messenger employed by a banking institution or express company;
- (e) to have and carry concealed by a justice of the supreme court in the first or second judicial departments, or by a judge of the New York city civil court or the New York city criminal court;
- (f) to have and carry concealed while employed by an institution of the state, or any county, city, town or village, under control of a commissioner of correction of the city or any warden, superintendent or head keeper of any state prison, penitentiary, workhouse, county jail or other like institution;
- (g) to have and carry concealed, without regard to employment or place of possession, by any person when proper cause exists for the issuance thereof; and
- (h) to have, possess, collect and carry antique pistols.

III. New York City Licensing Regime

In New York City, firearms licensing is controlled by the New York City Police Department (NYCPD). See also, Rules of the City of New York, Police Department, 38 R.C.N.Y. § 1.01 (2014). Residents of New York City who wish to obtain a firearm license must apply through the New York Police Department License Bureau at One Police Plaza in lower Manhattan. The choice of licenses are:

- (a) Rifle / Shotgun (38 R.C.N.Y. §3.01);
- (b) Gunsmith / Dealer (38 R.N.C.Y. § 4.01); and
- (c) Handgun (38 R.C.N.Y. § 5.01)

There are several different types of handgun licenses available. Under 38 RCNY § 5.01, these include:

- (a) Premises Residence (a restricted carry license issued for a specific location);
- (b) Premises Business (a restricted carry license issued for a specific location);
- (c) Carry Business (an unrestricted license that permits concealed carry on the person);
- (d) Limited Carry Business (a restricted carry license that permits concealed carry to/from specified locations on specified dates/times);
- (e) Carry Guard/Gun Custodian (restricted carry licenses for those employed as security guards or gun custodians); and

- (f) Special Carry—Business or Guard/Gun Custodian.

NYC Unrestricted Concealed Carry Licenses are valid throughout the rest of the state. NYC premises-only licenses are the licenses issued to average citizens who cannot show a need for self-defense greater than any another average citizen. Most licenses issued in New York City are for on-premises possession only, for self-defense within the home or business.

IV. Penalties

In the absence of a permit, simple possession of a firearm within one's home or place of business is a Class A Misdemeanor punishable by up to one year in prison, a \$1,000 fine, or both. N.Y. PENAL LAW § 265.01; § 60.01(3); § 70.15. Unlicensed possession of a weapon on school grounds is an E Felony (P.L. § 265.01-a), punishable by a term of imprisonment of up to four (4) years in jail. § 70.00(2)(e). Unlicensed/unregistered possession of three (3) or more firearms, of an assault weapon or a large capacity feeding device is a D Felony under § 265.02, punishable by a term of imprisonment of up to three (3) to seven (7) years in jail. § 70.00(2)(d). Unlicensed possession of five (e) or more firearms, is a C Felony under § 265.02, punishable by a term of imprisonment of up to three (3) to fifteen (15) years in jail. § 70.00(2)(c).

A partner of the firm in its White Plains office, Brian Stapleton's practice focuses on the defense of large-exposure products liability, labor law, wrongful death and other liability claims across the country. He engages in a significant amount of Second Amendment litigation, at both the trial and appellate levels, in New York and across the country. He also engages in extensive appellate advocacy in the courts of New York and the federal judiciary.

As a highly experienced trial attorney, he has obtained verdicts in over 100 cases and has tried numerous civil cases involving wrongful death, design and manufacturing defects, medical malpractice, and bankruptcy fraud. He has won high-profile criminal cases of murder and kidnapping, and has successfully defended complex multi-defendant RICO cases in the U.S. District Courts for the Districts of New York and Connecticut.

With several reported cases to his credit, he has successfully briefed and argued numerous appellate cases, most notably in *Illinois v. Dante Brown*.

This was a presentation in conjunction with the NYSBA CLE seminar "Security Concerns for Law Firms—What You Need to Know About Cybersecurity, Data Security, Office Security, and More."

Report on the Kenneth G. Standard Diversity Reception

By Matt Bobrow

On July 23, 2014, the Corporate Counsel Section held its annual celebratory Reception to honor the Kenneth G. Standard Diversity Internship Class of 2014 in the beautiful offices of Pryor Cashman LLP at Times Square in Manhattan.

From its beginning in 2006, the Kenneth G. Standard Diversity Internship Program has been one of the Corporate Counsel Section's signature programs. Over the nine summers that this program has been operated by the Section, more than 60 New York State law students who self-identify as "diverse" have served as summer interns in the law departments of upstate New York and New York Metropolitan Area-based businesses or non-profits under the Corporate Counsel Section's sponsorship so that they can experience in-house legal practice.

The program is named in honor of past New York State Bar Association President, Kenneth G. Standard, because of his commitment to initiatives designed to increase diversity in the legal profession as well as his initial and ongoing active support of the program. In part due to this program, NYSBA recognized the Corporate Counsel Section in 2013 and again in 2014 as a Section Diversity Champion. A major goal of the program is to create a network of Kenneth G. Standard Diversity Internship alumni and to help the alumni forge relationships that will foster greater diversity in corporate legal departments throughout New York State and elsewhere.

This year's honored host companies and their respective sponsored interns were The ACE Group (Ashley C. Dougherty and Neera Roopsingh, both of Albany Law School), AllianceBernstein (Susan Rhee of CUNY Law School), NYSTEC (Christina Arriaga of Albany Law School), Pepsi Co. (Jakarri Hamlin of New York University School of Law), Pitney Bowes (Alif Mia of Fordham Law School), Salesforce (Ryan M. Cloutier of Fordham Law School), and the Visiting Nurse Service of New York (Anita Yee of Brooklyn Law School). Representatives of each employer sponsor, the interns, our reception sponsor (Kaplan Bar Review), fellow Corporate Counsel Section members, and distinguished guests, including a number of New York State Judges and Justices as well as current and former Presidents of the NYSBA, Kenneth G. Standard among them, all attended the reception. While intended primarily to honor the host companies and the eight interns, the program also honored the entire NYSBA and the work its members have done to further diversity in the Bar.

In his remarks to open the ceremonial portion of the program by introducing NYSBA's current President, Glenn Lau-Kee, Tom Reed, Chair of the Corporate

Counsel Section, called attention to the fact that President Lau-Kee is NYSBA's first Asian-American President. He also reminded the attendees that the only African-American president before Kenneth G. Standard (2004-2005) was Archibald Murray (1993-1994), eleven years earlier. He pointed out that it was a shorter interval of eight years until the next and most recent African-American President, Seymour James (2012-2013), who was also present, was elected after President Standard.

During the subsequent award ceremony presided over by Dave Rothenberg, Chair of the Corporate Counsel Section's Diversity Committee, in the course of which both the employer sponsors and their respective law student interns received a handsome metal plaque to commemorate their participation, several of the interns made colorful remarks. One of the most memorable speeches was by Alif Mia, the intern at Pitney Bowes, who spoke of his father and the taxi he drove in New York City for 20 years. Alif said that his father would drive him through Midtown saying how Alif could work for any of the companies in any of the buildings (including the one we were in that very evening) so long as he did really well in school. Alif concluded by thanking all those who made the Kenneth G. Standard Diversity Internship possible and who helped make his father's promise come true.

The prevailing atmosphere throughout the reception was one of friendly support for the student interns, who readily engaged in conversations with the NYSBA members and others in attendance. This reporter observed a warm smile come over Ken Standard's face as he studied the plaques about to be awarded to the interns. A number of employer representatives and others in the room told me that their support for the program stems from the high quality of the interns and their ability to genuinely impress their managers. Many wished to hear more about the newest endeavors of the program's alumni. It was apparent that there is a real connection being made between these interns and their employers and other mentors who continue to support the program year after year. This was perhaps best exemplified when President Glenn Lau-Kee took some extra time at the end of the evening to enjoy a soda and a private talk with a several of the interns.

Now that the internships have ended for this year, each intern will be offered the opportunity to pair with a previous Kenneth G. Standard Diversity Internship alumni-mentor to help foster their continued development. All intern alumni are also eligible to participate in the Corporate Counsel Section's robust Kenneth G. Standard alumni program. This may include joining the Executive Committee of the Section and taking on a leadership role, as has been the case with our current Section Secretary,

Yamicha Stephenson, and Executive Committee Kenneth G. Standard Alumni Representative, Richard Kim. For more information about the Kenneth G. Standard alumni program, please contact Yamicha at yamicha.stephenson@gmail.com.

Section Member dues coupled with the generous support of our host companies and, in the case of the nonprofit internship, The New York Bar Foundation Fellowship funded by the Section, provide the necessary financial support for these internships. Many thanks go to Executive Committee member and former Section Chair David Rothenberg of Goldman Sachs, who contin-

ues to work tirelessly to ensure the continued success of the program.

Matthew Bobrow is a 3L Law Student at New York Law School where he is a Staff Editor for the *New York Law School Law Review*. He is participating in a training program with a Legal and Compliance rotations at Credit Suisse AG and is Law Clerking with Shafer Glazer LLP. Matthew is excited to be helping edit his first issue of *Inside*. Whenever possible, he is always looking for ways to contribute to the New York City legal community.

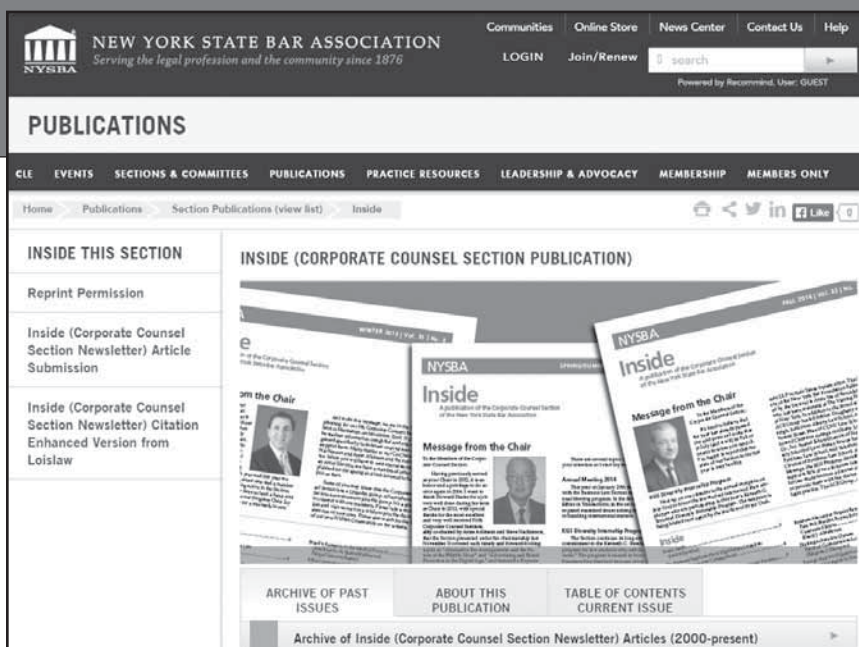
Inside (the Corporate Counsel Section Newsletter)

is also
available
online

Including access to:

- Past Issues of *Inside* (2000-present)*
- *Inside* (2000-present) Searchable Index
- Searchable articles from the *Inside* (2000-present) that include links to cites and statutes. This service is provided by Loislaw and is an exclusive Section member benefit*

*You must be a Corporate Counsel Section member and logged in to access. Need password assistance? Visit our Web site at www.nysba.org/pwhelp. For questions or log-in help, call (518) 463-3200.



Go to www.nysba.org/Inside



NEW YORK
STATE BAR
ASSOCIATION

The Boneyard

By Robert Cioffi

Basements typically do not invoke feelings of warmth or comfort—at least mine does not. It is dark, dingy and simply begging for a makeover. For the time being it is performing exceptionally well in its relegated role as a time capsule for the unwanted and forgotten relics of our lives. Boxes, furniture and assorted unknown objects are stacked together like a Rube Goldberg contraption gone horribly wrong. The creepy-crawlies, however, find refuge among this subterranean bramble despite the best stalking efforts of our two cats who remain futility fixed to flush them out.

In recent years, though, my wife and I had grown progressively uneasy with the micro urban sprawl growing in our cellar. Thus began the herculean effort to dismantle the mess while suppressing any emotion about the once-forgotten and now recently remembered things of the past. The cats, however, did not forget about their multi-legged tormentors and quickly seized the opportunity to exact justice for being teased for so long. But before they had time to lick their chops we had moved most everything to the driveway for the most spectacular extravaganza of the year: the mighty garage sale! That's right; it became our goal to get others to part with their cash for our old junk.

A business has its proverbial basement too. The "boneyard," as I like to call it, is usually that spare office or closet where the carcasses of old computers, machines and electronics are exiled. Their useful years are wholly spent yet there is no true finality for them. They are banished to a life (or is it a death?) in perpetual purgatory. Some people will visit this graveyard periodically to ponder a potentially different fate. Is there not some use to this stuff? Is there no one who would want or care for these neglected gadgets? Although most homeowners find success at unloading their surplus sundries, a business may not find it as easy to dispense with its derelict devices. Furthermore, what lays buried inside the electronic waste may be forgotten, but it should be remembered with tremendous gravity. The data these items contain could harm your business in a multitude of ways.

The natural instinct of most office managers is to task their computer guy with the mission to tackle this problem. They will know what to do with all that stuff, right? In many cases the answer is no, or the net result is plainly not worth their time and effort. In fact, the job is quite a burdensome chore very low on the priority list and riddled with problems. Let's examine them.

The first issue is environmental. We cannot (or should not) cram the dumpster with old computers, monitors and printers. They end up in landfills or are incinerated. Electronics are chock full of caustic and

dangerous chemicals including arsenic, mercury, lead and cadmium, to name a few. When burned, the PVC plastic found in most computers emits a harmful compound known as dioxin. All of these hazards are known to cause cancer, respiratory illnesses and reproductive problems. They are particularly dangerous because of their ability to traverse great distances through air and water systems, and are toxic even in small amounts. According to The Gartner Group, by 2008 over 2 billion PCs were sold since the first IBM PC rolled off production lines in the 80s, and over 1 billion are still in use today. So, what happened to the other billion? By 2013, the International Data Corporation ("IDC") estimated there were 1.8 billion cell phones in use and project there will be a total of 2.3 billion by 2017. Eventually all those devices will be considered trash. Countries like the United States, Japan and the European Union all have laws and systems to regulate and control the proper disposal of eWaste. But export systems are overwhelmed by the sheer volume of waste, and laws are mostly ignored. Furthermore, countries in Southeast Asia, such as China and India, do little to prevent the illegal import of eWaste because of the lucrative business opportunity. Aside from the dangerous elements, eWaste contains quite a number of valuable ones such as: gold, silver, copper, steel, zinc, aluminum, brass, plastics and other precious elements in rare-earth magnets.

The second problem eWaste represents is the potential for data leakage. Every business needs to be concerned about corporate or personal data falling into the wrong hands. Your old computer and electronics are likely to contain very important or sensitive files on storage systems like hard drives. Most business executives and IT managers are focused on the day-to-day compliance for regulations such as those concerning HIPAA/HITECH and Payment Card Industry matters. However, that tunnel vision can blind you from taking prudent steps once systems get powered off and disconnected. The data remaining behind still poses a threat. In addition to breaking the law, a sloppy error could mean the loss of business goodwill or reputation. For example, the recent hacker activity at Target and Home Depot has left some feeling nervous about continuing to transact with them.

If you are disposing of, or donating old equipment, you should take great care in making sure the data is either properly removed or destroyed before it leaves the building. This includes items like hard drives, flash drives, cell phones, backup tapes, copiers, printers, etc. Components such as these should be mechanically shredded to physically and permanently destroy the data. Just because the device is placed curbside does not mean a curious mind won't find it before the maw of the garbage truck does. If a device is donated, make sure your gift does not include more than you anticipated.

The third issue is an extension of the second. Most people I meet are genuinely willing to help others less fortunate. Although their heart is in the right place, sometimes their head is not. The reason most electronics end up in the boneyard is because they rightfully belong there. Nine out of ten times, their utility is gone. For decades the world of technology has been laser focused on manufacturing new electronic devices, yet no one has paid any attention to completing the circle of life. One obvious solution appears to be charity. But think about that notion for a moment. Here is an old PC that our office shoved into the bottom of a closet because it was super slow and was a few generations behind in terms of operating system and software. Perhaps even a few components were beginning to fail. Now I want to give this away to a church, a non-profit, an employee, a school, or some underprivileged kid. Are you really doing them a favor? Unfortunately, in order to participate in the globally interconnected digital society, you must have a vehicle that can at least keep up. The information super-highway has no speed limits but does impose minimum speed requirements. Standing still is hardly productive.

Is there hope? Indeed, hope is eternal. In my travels (and mainly because I am that computer guy tasked to do something about the boneyard), I have found a few outlets that can help.

First, there are commercial operations that will recycle your old equipment. The reputable ones achieve and maintain certifications such as e-Stewards or R2. Both are very similar and provide the consumer both assurance and peace-of-mind that eWaste is being disposed of in accordance with any applicable laws, and that items potentially containing data are physically destroyed. These organizations also likely confirm to the protocols and procedures outlined by the NIST 800-88 standard, and will offer Certificates of Data Destruction if requested. Ultimately, every business should perform its own due diligence to properly vet their vendors. The right certifications are a good starting point.

Second, although there is a wealth of online information, it is critical to trust your sources. The Basel Convention (www.basel.int) and the Basel Action Network (www.ban.org) are two related organizations at the forefront of eWaste disposal issues.

Third, a few years back I happened upon an impressive organization known as Per Scholas. Located in the South Bronx, its mission started in 1995 to put technology in the hands of disadvantaged students in low income areas. It has since grown into a local recycling powerhouse with designs on national expansion. It too will recycle systems in both manners: physical and responsible disposal, as well as refurbishing reusable equipment for training purposes, and as very low cost alternatives for students. It is certified at data destruction services and count major Wall Street firms among its clients. For a nominal fee you can bring your old computers to this organization, or for larger quantities you can arrange to have pickup at your office.

Finally, there are plenty of organizations that will accept your old CDs, DVDs and other magnetic media for recycling. Many will freely accept as much as you can ship them. The plastics are recycled and end up being re-used in things like car parts. A quick Google search will yield a ton of these outfits.

Despite how well we fared at our garage sale, the concept is powerful win-win-win. The seller gets to free himself from unessential items, and the buyer is likely to find herself a great bargain. But the subtlest and biggest winner is the landfill. Hopefully you now realize that dissolving your office boneyard is no longer a challenging or impossible job. Like the garage sale, everybody wins.

Robert Cioffi graduated Iona College in 1990 with a BS in Computer Information Science. After working at GE Capital for several years, he pursued an entrepreneurial calling and founded Progressive Computing with co-owner and college buddy, Ugo Chiulli. In his career at Progressive Computing, he has worked diligently to build the solid foundations on which his company stands: prompt, reliable, professional and expert service. Clients regard him as their Virtual Chief Technology Officer (vCTO) trusting in his 20+ years of business technology experience and pragmatic, decisive and creative personality. He is also widely known to be an expert public speaker on small business technology topics, an official advisor to vendors such as Microsoft, CCD Instructor and Lector for his local church, and serves on the Leadership Council of the Yonkers Strive Partnership.

Protecting Proprietary and Other Information When Using Third Party Vendors

By Kenneth C. Citarella

Do what you do best; have someone else take care of the rest. This is sound business advice under many circumstances. Subcontractors, business partners, vendors and joint ventures are all common manifestations of this maxim. When applied to the digital processing of your data, however, special care must be taken. Attorneys must understand these risks to properly counsel their clients, as well as to protect their own firm and fulfill their ethical obligation to protect the confidentiality of client information.

The Nature of the Third Party Threat

Before discussing how to protect yourself and your clients, we must understand the many ways in which third parties pose a risk to the sensitive information belonging to you and your clients. Consider these recent examples from the business world:

- The Target data breach that exposed the information of an estimated 70 million customers in late 2013 was possible because of a series of security lapses within Target. The initial entry point of the attack, however, was through Target's HVAC contractor who had authorized access to Target's network.¹ That access permitted the vendor to manage the HVAC systems in Target's facilities remotely, but also granted the intruder access to Target's Point of Sale terminals.²
- In May 2014, Lowe's, the home improvement chain, blamed a data storage vendor for a possible breach of its employees' personal data. The vendor backed up the employee data, including names, addresses, dates of birth, social security numbers and driver's licenses, onto a server that was readily accessible over the Internet. A mistake, not an attack, but with similar results for the individuals affected.³
- In June 2014, AT&T notified an undisclosed number of its mobile customers that "... employees of one of our service vendors violated our strict privacy and security guidelines by accessing your account without authorization..."⁴ Strong privacy policies are not always enough to deter misconduct by a vendor's employees.

An intrusion through a vendor, a vendor's mistake and a deliberate policy violation by a vendor's employee are three different variations on a common theme: every person who has access to your data creates a risk.

Lest anyone suggest that the government is any better at controlling third party risk, keep Edward Snowden in mind. Strip away the political, international and legal issues generated by his disclosures, and at the heart of the story we have a trusted employee of a trusted vendor breaking all of the rules of the data owner. Consider these other recent stories as well:

- On August 29, 2014, the Colorado Secretary of State wrote to the Governor stating that "thousands of employees' and contractors' personal information" was exposed to unauthorized access on a state system.⁵
- The U.S. Government Accountability Office ("GAO") reported in August 2014 that it had reviewed six federal agencies to determine their effectiveness in assessing whether their contractors had established security and privacy controls for government data. GAO stated that five of the agencies "were inconsistent in overseeing the execution and review of those assessments, resulting in security lapses."⁶

Sadly, none of these examples is unique. According to a 2013 study of 450 data breaches worldwide, 63% were linked to a third party involved in system administration.⁷ The third party vendor had actually introduced security loopholes "easily exploited" by intruders. One of the authors commented that the evaluation process for IT vendors tends to focus on cost and services rather than security.⁸

Sample Cases Involving Third Party Incidents

Of course, data breaches generate litigation, often class action suits by plaintiffs whose personal information was exposed due to a data breach. While courts seem to be consistently ruling that exposure alone is not enough harm to create a plaintiff class, suits keep coming. For our purposes, the following cases illustrate the types of underlying breaches that have generated court cases.

Plaintiff Cumis Insurance Society paid millions of dollars to credit unions it insured against losses resulting from a data breach due to the alleged negligence of Merriam Bank Corporation and its agents.⁹ One of those agents maintained data from the magnetic strips of the credit cards for longer than needed and also failed to adequately protect the data.¹⁰ This is an excellent example of a third party's technical failing leading to a data breach.

Payment Card Industry ("PCI") standards set a security mandate for any entity involved in processing

transactions. Not all processors are compliant. The still infamous Heartland data breach is an excellent example. This incident, which exposed the records of approximately 130 million consumers, was due to an intrusion into its system, which was not PCI compliant.¹¹ Similarly, between December 2009 and December 2010, cyber criminals installed malware on the computers of Genesco, Inc., a sportswear retailer.¹² The program read unencrypted data as transactions were transmitted from Genesco to its merchant banks. VISA, pursuant to its agreement with those banks, assessed the banks more than \$13 million for failing to ensure that Genesco was PCI compliant.¹³

A case that started as a simple break-in to a motor vehicle actually combines several issues we have identified. In September 2011, a thief stole a car's GPS system, radio and several data tapes.¹⁴ Those tapes belonged to a federal vendor and contained personal information and medical history on 4.7 million members of the U.S. military and their families.¹⁵ The vendor's employee probably thought the tapes were perfectly safe in his locked car, and the thief certainly had no knowledge of what they contained. Nonetheless, the conduct of a third party vendor created risk for the government and for millions of individuals.

Ethical Considerations for Attorneys

Rule 1.6(a) prohibits a lawyer from revealing a client's confidential information and 1.6(c) requires exercising reasonable care that "employees, associates, and others whose services are utilized" do not reveal either.¹⁶ Whether storing client information on an office computer or in the Cloud (a fancy word for off-site or remote storage), third party cyber security is now a front-and-center ethical obligation.

One case depicts the substantial risks. Three employees at a law firm used Dropbox (a remote storage application) to transfer copies of approximately 78,000 documents out of the firm just before they quit and went to another law firm. They then altered the copies in their Dropbox accounts and synched them to the first law firm's network so that the originals were altered with incorrect information.¹⁷ Why were the employees permitted to access Dropbox from the law firm's system? Why was a bulk transfer of documents possible? Almost certainly no one understood that such risks existed, or would have appreciated the dangers if informed of them. That is a risk lawyers can no longer take. Indeed, the few ethical opinions that have been published on related issues make it clear that an attorney must use "reasonable care to ensure that the system is secure and that client confidentiality will be maintained."¹⁸

So, what exactly satisfies the standard of reasonable care? After all, no system is foolproof. Fortunately, the decisions do provide some guidance:

- Have an enforceable obligation that the vendor will preserve confidentiality;¹⁹
- Perform your due diligence on the vendor;²⁰ and be sure the vendor has adequate security and recovery procedures;²¹
- Be sure the vendor can completely remove data and export it to another vendor if needed;²²
- Periodically reconfirm all of the above;²³
- Consider obtaining the client's consent, perhaps in the retainer agreement;²⁴
- Use encryption;²⁵ and
- Establish your own data management policies and procedures;²⁶ and enforce them.

Conclusion

Almost every law firm and almost every client will have some dependency on third party vendors for the storage and processing of information that is confidential to employees, clients and perhaps the public at large. The ethical obligation to be competent²⁷ certainly embraces some understanding of the risks third parties represent to a law firm's and its clients' data. Attorneys must understand the risks, and guide their clients through contractual and insurance-related issues to minimize them.

Endnotes

1. U.S. Senate Committee on Commerce, Science, and Transportation, A "Kill Chain" Analysis of the 2013 Target Data Breach 4 (2014).
2. *Id.* at 9.
3. Fred Donovan, *Third-party vendor behind possible Lowe's data breach*, <http://www.fierceitsecurity.com/node/1126> (last visited Oct. 6, 2014).
4. Jeff Goldman, *ATT Customer Info Exposed by Third Party Data Breach*, <http://www.esecurityplanet.com/network-security/att-customer-info-exposed-by-third-party-data-breach> (last visited Oct. 7, 2014).
5. Chris Halsne & Chris Koeberl, *Records: State's new computer system puts thousands of employees' personal info at risk*, FOX31 Denver, <http://kdvr.com/2014/09/15/social-security-numbers-exposed-by-states-new-computer-system> (last visited Oct. 7, 2014).
6. U.S. Gov't Accountability Office, GAO-14-612, *Agencies Need to Improve Oversight of Contractor Controls* (2014).
7. Warwick Ashford, *Bad outsourcing decisions cause 63% of data breaches*, <http://www.computerweekly.com/news/2240178104/Bad-outsourcing-decisions-cause-63-of-data-breaches> (last visited Oct. 7, 2014).
8. *Id.*
9. *Cumis Ins. Society, Inc. v. Merrick Bank Corp.*, No. CIV 07-374-TUC-CKJ, 2008 U.S. Dist. LEXIS 78451, at *1-2 (D. Ariz. 2008).
10. *Id.* at *2.
11. *In re Heartland Payment Sys., Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 575 (S.D. Tex. 2011).
12. *Genesco, Inc. v. Visa U.S.A., Inc.*, 296 F.R.D. 559, 561-63 (M.D. Tenn. 2014).

13. *Id.*
14. *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 2014 U.S. Dist. LEXIS 64125, at *3 (D.D.C. 2014).
15. *Id.*
16. *New York State Rules of Professional Conduct*, Rule 1.6.
17. Ericka Chickowski, *Slide Show: 8 Egregious Examples Of Insider Threats*, <http://www.darkreading.com/vulnerabilities---threats/slide-show-8-egregious-examples-of-insider-threats/d/d-id/1139493?> (last visited Oct. 7, 2014).
18. New York State Bar Association, Ethics Opinion 842 (September, 10, 2010); New York State Bar Association, Ethics Opinions 940 (October 16, 2012).
19. New York State Bar Association, Ethics Opinion 842 (September, 10, 2010).
20. New York City Bar Association, Committee on Small Law Firms, *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations* (2013).
21. New York State Bar Association, Ethics Opinion 842 (September, 10, 2010).
22. *Id.*
23. *Id.*
24. New York City Bar Association, Committee on Small Law Firms, *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations* (2013).
25. *Id.*
26. *Id.*
27. *New York State Rules of Professional Conduct*, Rule 1.1.

Kenneth Citarella is Managing Director for Guidepost Solutions' Investigations and Cyber Forensics practice. He joined Guidepost Solutions in 2010 as a Project Manager to investigate fraudulent claims for the Gulf Coast Claims Facility in its administration of the \$20 billion BP compensation fund. Mr. Citarella also worked as part of the Guidepost Integrity Monitor team in the New York City Rapid Repair program overseeing Superstorm Sandy-related reconstruction on Staten Island. Prior to joining Guidepost, Mr. Citarella worked with a commercial litigation law firm and the Corporate Investigations Division of Prudential. Mr. Citarella had a distinguished 28-year career as a white-collar and computer crime prosecutor in the Westchester County, New York District Attorney's Office, which he concluded as Deputy Chief of the Investigations Division. Mr. Citarella is a Certified Fraud Examiner, Certified Information Privacy Professional, and an Adjunct Professor of Law at New York Law School, where he teaches a cybercrime course. He frequently lectures before professional, legal, academic, corporate and community groups on computer crime and fraud-related issues. In 2013, Mr. Citarella began a three-year term on the New York City Bar Professional Responsibility Committee. In 2011, he received the Lifetime Achievement Award from the High Technology Crime Investigation Association.

NYSBA's CLE Online

))) ONLINE | iPod | MP3 PLAYER

Bringing CLE to you... anywhere, anytime.

NYSBA is proud to present the most flexible, "on demand" CLE solutions you could ask for.

With **CLE Online**, you can now get the valuable professional learning you're after

...at your convenience.

- > Get the best NY-specific content from the state's **#1 CLE provider.**
- > Take "Cyber Portable" courses from your laptop, at home or at work, via the Internet.
- > Download CLE Online programs to your iPod or MP3 player.
- > Everything you need to obtain full MCLE credit is included **online!**



Come click for CLE credit at:
www.nysbaCLEonline.com



Features

Electronic Notetaking allows you to take notes while listening to your course, cut-and-paste from the texts and access notes later – (on any computer with Internet access).

Audio Seminars complement the onscreen course texts. You control the pace, and you can "bookmark" the audio at any point.

Bookmarking lets you stop your course at any point, then pick up right where you left off – days, even weeks later.

MCLE Credit can be obtained easily once you've completed the course – the form is part of the program! Just fill it out and mail it in for your MCLE certificate.

Being Prepared When the Cloud Rolls In

By Natalie Sulimani

With each new technological advance comes at least one new word, if not a whole new language. It seems as if once you get a handle on one term there is yet another one to learn – crowdfunding and crowdsourcing, to name a few. And then there is social media, which should not be confused with social networks, of course. This is all in the spirit of service to technology and innovation. But none strike more fear in the heart of attorneys lately than the ubiquitous term “cloud computing.” What is the cause of the shudder you just may have felt run through the legal profession? Maybe the discomfort comes from the natural desire in the field of law to control as much of our client’s situation as possible, and cloud computing is an environment that we, as attorneys, cannot ultimately control. It is, by its very nature, in the hands of someone else. Hopefully, you have found a trusted Information Technology vendor to manage your part of the cloud.

But, while with technology the players and the terminology may change, what does not change is an attorney’s ethical obligations. We have a duty to maintain confidences, a duty to remain conflict free in our representations and, of particular interest to me lately, a duty to preserve.

The lesson has been taught, and sorely learned, that files must be backed up. Hard drive failures are, unfortunately, a reality. So, you back up to an external hard drive. Except the unwritten rule of the cyberspace is hard drives always fail. Always. Recently, the onslaught of natural disasters, the latest being Hurricane Sandy on the East Coast, has taught some lawyers a very harsh lesson. Redundancy is important. Maintaining files in multiple locations is a must. How many files were lost due to flooding or a server going underwater? How many attorneys were unable to access their files because of these or other similar catastrophes? If it was even one, then it was too many. And worse yet, there is no reason for such things to happen.

Early in my solo career, I had a breakfast networking meeting with an attorney from a midsize firm and the discussion turned to the topic of working from home. Now, technically, I do not have a virtual law firm, but I do consider myself mobile as an attorney. I think most of us do. Technology allows us to do so. Moreover, the amount of work necessitates that we work remotely. Clients expect you to be available on their schedule, and worse yet, clients or opposing counsel may live in a different time zone. Not everyone exists on Eastern Standard Time. So, I casually asked, “How do you manage your work from home?” The answer was, “I email my files to myself.” I followed up with, “Okay. To your firm’s address?” The response that mentally gave me pause was, “No, personal email address.” There seemed something wrong about this, but more on that later.

Opinions regarding maintaining confidentiality are numerous, frequent and, as we move forward technologically, the subject keeps returning like a bad penny. We all

know that we need to maintain confidentiality. But the challenge as we progress may be to understand new technology so that we are able to use it to be more efficient, while at the same time being confident that we are maintaining client confidentiality.

History and the Ethics Trail to Cloud Computing

If you have attended seminars on cloud computing, then you may know that the first iteration of the cloud was voicemail. Answering machines were replaced with voicemail, which meant that your messages were stored on a remote server that required you to use a code to retrieve them. Although this was a shift in where personal and official information was stored, I cannot remember anyone wondering whether this would be an issue of confidentiality or otherwise. The result was everyone chose voicemail over answering machines for the convenience of listening to messages anywhere.

The next step in cloud computing came in the form of third-party email providers like Gmail, Yahoo, MSN, Hotmail, AOL, and others. These services stored our communications on remote servers in any number of locations, but most important, all this information resided in the cloud. Again, almost everyone is happy to access his or her email from anywhere without fretting over the fact that all our words and thoughts are floating out there in the cloud.

So how do the courts view this use of the cloud? An opinion rendered in 1998 in New York State said that a lawyer may use *unencrypted* email to transmit confidential information since it is considered as private as any other form of communication. Unencrypted means that, from point to point, the email could be intercepted and read. The reasoning was that there is a reasonable expectation that e-mail will be as private as other forms of telecommunication. However, the attorney must assess whether there may be a chance that any confidential information could be intercepted. For example, if your client is divorcing his or her spouse, an email that both spouses share, or even an email to which the non-client spouse has access, should not be the method of communication. The attorney must seek alternate methods of communicating.

Gmail did add an extra twist, which other email service providers quickly copied. As a “service” to you, email service providers started to scan emails in order to provide you with ad content. They would scan keywords in your email and provide relevant advertising. For instance, if you were discussing shoes in an email, the email service provider would tailor ads when you were in the email inbox and you would now be receiving advertisements for Zappos or any other shoe vendor. After all, nothing is better than a captive audience.

So, the question now becomes whether a lawyer can use an email service that scans emails to provide computer-generated advertisements. The New York State Bar Associa-

tion opined in Opinion 820 (2/8/08 (32-07)) that, yes, it was okay, since the emails were scanned by machine and not by human eyes. If the emails were read by someone other than sender and recipient, the opinion would have certainly been different.

And now to the topic at hand: storing client files in the cloud. Through services like Dropbox, Box.com, Rack-space, Google Docs, and others, an attorney can add to his or her mobility and efficiency by storing client files online. Although I know there is a lot of debate surrounding this practice, I do not see how it is very different from storing client files off-site in a warehouse. In the cyberworld, electronic files are held by a third party on a secure remote server with a guarantee that they will be safe, and only authorized persons will have access. In the brick-and-mortar world, paper files are held by a third party in a warehouse with the same guarantees. Both are equally secure and equally liable to be broken into by nefarious agents bent on getting to the diligently hidden confidential information. Again, the technology might change, but the principles are the same. One should not be more or less afraid of one method of storage over the other.

A number of state bar associations have been grappling with the issue of cloud computing and the ethical issues it raises; these include North Carolina, Massachusetts, Oregon, Florida, as well as our esteemed New York State Bar Association. However, surprisingly, to date only 14 of the 50 states have opined regarding use of cloud computing in the legal profession. One would think more would have joined the fray in giving its lawyers some guidance.

The American Bar Association amended its model rules last year, perhaps as a beacon to other bar associations, but certainly as a guide for other states.

Model Rule 1.6 holds:

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Across the board, opinions are cautious about using cloud computing in the practice of law, but there is nothing about it that could be called unethical. The ethical standard of confidentiality is *reasonable efforts to prevent disclosure*. The question, therefore, lies in what is considered reasonable efforts.

Rule 1.6(a) of the New York Rules of Professional Conduct states that “[a] lawyer shall not knowingly reveal confidential information...” and, at Rule 1.6(c) goes on to say that “[a] lawyer shall exercise reasonable care to prevent the lawyer’s employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client.”

It is safe to assume that Rule 1.6(c) imposes the obligation for lawyers to use reasonable care in choosing their cloud computing and/or IT vendors, but indeed those lawyers may take advantage of the cloud and employ

those who provide and manage those services in good conscience.

In fact, in September 2010, the New York State Bar Association issued Ethics Opinion 842 regarding the question of using an outside storage provider to store client information. The question that was asked of the New York State Bar Association was whether a lawyer can use an online storage provider to store confidential material without violating the duty of confidentiality.

So What Exactly Is the Cloud?

To understand what the issue is and why it may pose a problem, it is best to understand what it means to store information in the cloud. A cloud, in its simplest terms, is a third-party server. The server in which the information is stored is neither on the law firm’s premises nor owned by the law firm. The law firm’s IT person or department does not maintain where the database is stored in any way. It is in the hands of a third party offering a service.

An internal storage system is a closed circuit, meaning there is a direct line from your desktop to the firm’s server. Absent hacking, the information is controlled internally. Once removed from this closed system and stored in the cloud, your information may be more vulnerable because you have now created access points in which others may gain access to that data. To illustrate, data will now flow out on the Internet and beyond your control to get to the remote server where it is housed. However, encrypt the data and you have limited the exposure. As stated above, once encrypted it would take a nefarious and willful mind to be able to read what you are sending into the cloud.

Why Should You Move Your Data to the Cloud?

There are many reasons why you would want to move to the cloud and many reasons why it is prudent to move your storage to the cloud. To begin with, properly using cloud computing in the storage of client information reduces the possibility of human error. Emailing files to yourself, transferring them to a thumb drive, storing client files in offsite warehouses, to name a few, are all steps that introduce and increase the chance for human error. Email to your personal email account runs the risk that your family would access your email at home, thumb drives get lost, people break into warehouses and natural disasters happen that can destroy files. Cloud computing, by contrast, puts your files in the hands of competent IT professionals who will secure your information and provide the necessary redundancy so that if a server goes down your files will live on and be available when you need them from another server. Their major, if not sole, purpose (and the reason you pay them) is to safeguard your files and ensure that you will always have access to them when necessary, so they are highly motivated to do it well and properly.

In March 2012, the Federal Trade Commission (FTC) issued a report titled *Protecting Consumer Privacy in an Era of Rapid Change*. While attorneys may be subject to higher standards in keeping client confidences, I think this is a

good guide in understanding the technology and best practices associated with it.

The FTC report recognized that businesses are moving to the cloud because it improves efficiency and is cost effective. However, the overarching concern is privacy. The FTC recommended overall guidelines for technology and consumer data. In particular, there are four recommendations that businesses should follow:

- *Scope*: Define what information is stored.
- *Privacy by Design*: Companies should promote privacy in their organizations.
- *Simplified Choice*: Simplify choice so that the customer is able to choose how information is collected and used in cases where it is not routine, such as order fulfillment.
- *Greater Transparency*: Companies should be transparent in their data practices.

Using these guidelines, what are best practices for attorneys?

- Consider what client information you will store in the cloud.
- Privacy is easy to ensure, attorney-client privilege should be maintained.
- Determine what information you will share with your clients. For example, will you share their case files with them? You can pick and choose what you share with your clients in the cloud for greater collaboration and reduction of emails going back and forth with attachments. They can upload their data in a secure environment, and you can share information in a secure, password-protected environment where you can ensure that only a specific client or clients have access.
- Choice and transparency go hand in hand. While it is the attorney's best judgment in deciding how to reasonably protect client information, you should make your client aware that you are using these services. Build it into your retainer. If, for any reason, your client objects, you will know and can deal with the reasons why right at the beginning. It may take just a short conversation about the confidentiality, reliability and ease of the cloud to assuage any fears or concerns.
- Finally, have a breach- notification policy in place. This is not just for your corporate clients; any client whose information is in the cloud should be notified of and subject to this policy.

Now that I have you on board with moving your files to the cloud, consider that you need to exercise "reasonable care" in choosing a cloud provider. New York State Bar Association Ethics Opinion 842 offers some guidance:

- Ensure that the online storage provider has an enforceable obligation to preserve confidentiality and security and will notify you of a subpoena.

- Investigate the online storage provider's security measures, policies, recoverability methods and other procedures.
- Ensure that the online storage provider has available technology to guard against breaches.
- Investigate storage provider's ability to wipe data and transfer data to the attorney should you decide to sever the relationship.

Read the Terms of Service and, when you can, negotiate with the cloud vendor. Cloud vendors update their policies and may be willing to change their practices to meet the needs of their (and your) clients. If you have concerns and/or specific needs, contact the vendor, and if it is unwilling to change its practices, go somewhere else. Frankly, there are many online storage providers so be discerning when it comes to client data.

While utilizing an online storage provider, consider its encryption practices. Will your data be stored encrypted? Will you encrypt the data enroute to the online storage? And who has access while it is being stored? Also, if the online storage provides access on mobile devices, just as you would your computer, laptop, tablet and mobile phone, add security by password protecting the online storage's mobile app. After all, just as in the non-cyber world, a big threat to effective storage is human error. Therefore, it is of utmost importance that you know how to remotely wipe the data if your device is lost or stolen. One aspect of mobile storage to be aware of is that when you download client data to your mobile device, it may be downloaded to your Secure Digital or "SD" card. Whether you want this is something to consider; take steps to avoid it, if desired. This is an example of the importance of understanding how the technology works, understanding where problems, such as interception, may occur, and ultimately how to take steps to avoid them. Education is key.

In short, the advantages of cloud computing as outlined in this article make it a perfect complement to an effective and successful law practice. There is little difference in the potential ethical issues or any other such problems that exist in the cloud and in the brick and mortar world of physical offsite storage of clients' files. Rather than running away from this new technology, it would be better to embrace it by learning more and making wise decisions that will minimize potential pitfalls down the road, while at the same time increasing the ease and usefulness of client communication and interaction.

Natalie Sulimani (natalie@sulimanilawfirm.com) is the founder and partner of Sulimani & Nahoum, PC. She is engaged in a wide variety of corporate, employment, intellectual property, technology, Internet, arbitration and litigation matters. She counsels both domestic and international clients in an array of industries. Ms. Sulimani earned her LL.B. from the University of Manchester at Kiryat Ono, Israel. This article first appeared, in a slightly different format, in the Fall 2013 issue of *Inside*, a publication of the NYSBA's Corporate Counsel Section.

Cybersecurity Due Diligence in Corporate Acquisitions

By Joseph V. DeMarco and Jeremy Apple

I. Privacy and Security Due Diligence for Corporate Acquisition and Venture Capital Firms

Recent rapid advances in technology over the last decade have transformed every aspect of our commercial and personal lives. Beyond the everyday use of smart-phones and mobile computing technology that has transformed communications, nearly all U.S. small businesses (98%) now use wireless technologies in their operations, with two-thirds (66%) indicating they could not survive without them.¹ As access to the Internet and interconnectivity reaches new heights across the world, commercial enterprises have embraced this technology as both a commodity and a locomotive for daily operations in a global economy. So too have Venture Capitalist (VC) firms and other corporate acquirers, from adopting applications such as commercial acquisition research and analysis to supporting everyday business operations.

Increasingly, corporate acquirers have also—sometimes through painful lessons—grown familiar with many of the common cybersecurity risks posed to organizations. These include network intrusion and disruption by outsiders in addition to the well-known “insider threat.” Importantly, this is not a “high-tech” issue, since *every* company collects and maintains data—and the value of such data forms a key component of a company’s assets. These factors can, and often do, have real bottom-line financial and public relations implications, as Facebook and other companies have learned the hard way, often repeatedly. In short, information privacy and security failures have real and sometimes devastating legal and commercial implications when not adequately addressed. Home Depot proved this.²

Of course, legal liabilities are but one form of harm that can affect companies that get privacy and security issues “wrong.” As was evident with the 2011 Epsilon e-mail data theft and resulting Congressional hearings, even where a company is the victim of organized cyber-criminal hacking, legislators are not shy about publicly “blaming the victim.”³ Not surprisingly, customers and investors are also quick to penalize companies perceived as lacking appropriate security. And, as more and more companies become sensitized to these issues and insert undertakings into contracts with business partners to prevent them, the consequences of data privacy and security laxity grow exponentially. Thus, sound internal cybersecurity practices are now central to the competitiveness of modern corporate acquirers, supporting financial stability through bolstered commercial reputation and increased operational efficiency.

While some corporate acquirers have sophisticated IT infrastructure and control of their systems (though many do not), the targets of acquisitions by VC firms often are not so cyber-resilient. Although cyber threats by outside hackers and current or former employees plague these companies as well, these businesses are less likely to have significant real or human capital invested in sufficient information privacy and security practices. Thus, the businesses that are subjects to investments or acquisitions may not be well suited to prevent cyber threats or maintain adequate information privacy and security protections. As a result, the cybersecurity risks faced by these organizations have the potential to disrupt or significantly influence acquisitions in numerous ways. Specifically, cybersecurity and information privacy practices have significant implications for corporate acquirers in the related areas of (a) acquisition due diligence, and (b) successor liability, and (c) regulatory enforcement. It is therefore imperative that such firms make information privacy and security matters a priority in their due diligence.

II. Cybersecurity Issues for Corporate Acquirers

A. Pre-Acquisition Due Diligence

Pre-acquisition due diligence is a familiar concept. Typical due diligence analyzes compliance with laws such as the U.S. Foreign Corrupt Practices and UK Bribery Act, Patriot Act, as well environmental law and other areas of compliance. Even apart from compliance imperatives mandated by law, however, savvy investors and acquirers want to know *what* they are purchasing. Indeed, accounts receivables due diligence is one example of diligence performed even though the “quality” of a company’s receivables may not implicate compliance with any federal or state statutes.

Like many U.S. businesses across various industries, corporate acquirers have acknowledged the emerging threat of insider misappropriation and fraud to some extent. The recent increase of criminal and civil matters involving theft of company intellectual property, confidential information, or personal identifying information is one byproduct of this growing trend.⁴ Studies by organizations like the Carnegie Mellon University Software Engineering Institute’s CERT Division and the United States Secret Service National Threat Assessment Center have helped organizations define and recognize the varying motivations and risks posed by current and former employees that harm U.S. businesses.⁵ Importantly, the varied motivations of insiders seeking to harm an organization range from pure potential financial gain, to commercial competitive advantage, to simple revenge.⁶

While VC firms are sometimes aware of cybersecurity risks, they typically focus, however, on combating *internal* threats of misappropriation or sabotage by current and former employees. Accordingly, they tend to emphasize the security of information stored in their network from misuse by current and former employees. Equal focus, however, must be placed on *external* threats to VC firms *and* the companies in which they invest. Hackers and other intruders present an array of additional complications for businesses seeking to secure digital assets and protect confidential information. External cyber-threats include wrongdoers seeking financial, personal or corporate information that can be used for an advantageous purpose. From confidential work-product and sensitive business data to network and system architecture information, the loss of internal data can present a significant risk to a parent or acquiring company if misappropriated.

B. Successor Liability and Regulatory Enforcement

Beyond the loss of its own confidential or proprietary data, corporate acquirers should also be concerned with regulatory liability under principles of successor liability.

Successor liability is, of course, nothing new in government enforcement actions. Massive fines and penalties have been imposed upon companies under the Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. (FCPA) and export control area under this principle of corporate responsibility. In an era of vigorous data privacy and security enforcement by the Federal Trade Commission (FTC) and State Attorneys General, as well as mass data-breach litigation, no company can fail to be concerned about its information and privacy security risk profile—or the companies that it does business with or acquires.

Understanding and minimizing cybersecurity risks are especially important VC firms whose business it is to invest in other companies. Any entity seeking to acquire or investing in another company simply can no longer “hope for the best” when it comes to the data privacy and security history of a target company. Notably, the FTC—the federal agency chiefly responsible for enforcing the nation’s emerging privacy laws—has since 2008 asserted in publicly filed litigation that where a data breach straddles an acquisition, both the target company *and* the acquiring company bear responsibility for the breach, even where the breach began prior to the acquisition and was not discovered until afterwards.⁷ More recently, a major Internet behavioral advertiser almost went bankrupt because it acquired a company that had engaged in questionable data collection practices. When asked how this could have occurred, the head of compliance at the acquiring company said that those questionable data collection practices were “missed in the due diligence.”

III. Achieving Cyber Best Practices in Acquisition Transactions

A. Assessment

What can VC firms do to protect themselves and their acquisitions from the threats presented above? Organizations such as VC firms must take precautionary measures on several fronts, including mitigating insider threats, external intrusions, as well as inadvertent loss or disclosure. While no outright formal industry-specific standards exist to benchmark VC cybersecurity initiatives, corporate acquirers can look to subject matter experts (ideally, legal counsel, for privilege purposes) well versed in cybersecurity counseling. Expert counsel can also assist such firms in aligning their cybersecurity and information privacy programs to the guidelines and benchmarks in various financial sector standards laws as Gramm-Leach-Bliley Act and private standards such as the Payment Card Industry Data Security Standard (PCI DSS).⁸

Corporate acquirers should also adapt their governance strategies to confront cyber-risks of acquired-entities with thorough, size and subject-matter appropriate due diligence. While a comprehensive assessment may not be warranted for certain transactions, performing even a basic review of the cybersecurity risks faced by the company being acquired will provide essential insight for the such firms to develop the optimal strategy to mitigate those risks. Cybersecurity experts can provide acquirers with a clear understanding of the true nature of an acquired entity’s risk, which may be leveraged in the acquisition. In short, VC firms can work to address particular areas of risk identified by experts, and perform targeted analysis that will maximize the corporate acquirer’s return on investment (ROI) in that due diligence.

B. Compliance Review

Beyond retaining an expert to perform a cybersecurity risk assessment, corporate acquirers must also ask essential *legal* questions of the company being acquired. Just as no company can effectively disclaim liability for contaminants in the ground of real property that it owns or acquires (or FCPA liability), no company can avoid the consequences of data and privacy problems “in the ground” at an acquired company. In an era of blossoming regulatory actions, class action litigation, front-page headlines regarding data breaches, supposed online tracking of consumers, and finger-pointing all around when a data mishap or “problematic” use of technology comes to light, avoiding legal exposure and reputational risk is of paramount importance.

Acquirers must therefore consider the legal implications surrounding each type of data that the target company stores in its systems and databases. For example, certain state and federal laws and regulations will govern certain internal protocols for the storage, transmission, or disposal of certain types of information. Corporate acquirers should consider the nature and location of the infor-

mation being both *stored* and/or *used* by the acquiring company. An entity will be subject to certain laws or standards if it stores or maintains certain personal, financial or other confidential information about employees, customers, or third party vendors and partners. Compliance with those regulations and standards will likely depend on the security measures implemented at the physical and logical locations where such information is stored.

Practically, corporate acquirers can formalize the privacy and security practices of a target company identified during diligence assessments and develop a Written Information Security Policy (WISP) and Cyber Incident Response Plan (CIRP) which reflect industry standards and practices. The exercise of creating formal policies surrounding the target firm's security and privacy practices can provide significant assurances that particular information and security standards are met by the target company. Furthermore, where the target company's practices fail to meet industry standards or best practices, acquirers may have additional leverage in certain transactions.

C. Let Industry Standards and Best Practices Be Your Guide

In the end, of course, information privacy and security is not just about risk analysis and minimization. *Even more fundamentally, it is about helping VC firms deepen their understanding of valuation.* For even if a company has not had any data spills, and is not engaging in illegal data collection practices (and the line between lawful and unlawful uses is often quite hard to discern), certain uses of technology are unpopular with business partners and consumers even where they are arguably properly disclosed and permissioned. Similarly, acquirers must also examine their *own* practices and amend their WISP and CIRP to reflect additional cybersecurity or privacy issues emerging in the course of its transactions. Knowing what data a company has and how it obtained that data is, therefore, literally to know what you (a) own, (b) are selling, and (c) are buying. And this knowledge can, when properly analyzed, play a critical role in pricing and valuation. Put simply, it should be a tool in every corporate acquirer's negotiating tool box.

Endnotes

1. See AT&T Small Business Technology Poll (2013), available at <http://about.att.com/mediakit/2013techpoll>.
2. See, e.g., Jaikumar Vijayan, *Data Shows Home Depot Breach Could Be Largest Ever*, COMPUTERWORLD (2014), available at <http://www.computerworld.com/article/2601349/data-shows-home-depot-breach-could-be-largest-ever.html>; Trefis Team, *Home Depot: Could The Impact Of The Data Breach Be Significant?*, FORBES (Sep. 24, 2014, 1:39 PM), <http://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/>.
3. See *Sony and Epsilon: Lessons for Data Security Legislation: Before the Subcomm. on Manufacturing, Commerce, and Trade*, 112th Cong. (2011), available at <http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg71258/html/CHRG-112hhrg71258.htm>.
4. See Stephanie Overby, *Hacked: The Rising Threat of Intellectual Property Theft and What You Can Do About It*, CIO.COM (July 30, 2007, 8:00 AM), <http://www.cio.com/article/2438356/risk-management/hacked--the-rising-threat-of-intellectual-property-theft-and-what-you-can-do-about-i.html>.
5. See, e.g., ANDREW P. MOORE, ET AL., THE "BIG PICTURE" OF INSIDER IT SABOTAGE ACROSS U.S. CRITICAL INFRASTRUCTURES, CARNEGIE MELLON CERT PROGRAM (2008), available at <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8703>; GEORGE SILOWASH, ET AL., COMMON SENSE GUIDE TO MITIGATING INSIDER THREATS, 4TH ED., CARNEGIE MELLON CERT PROGRAM (2012), available at <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1669&context=sei>.
6. Silowash, *et al.*, at 4.
7. See *In the Matter of Reed Elsevier Inc. et al.*, File No. 052-3094, No. C-4226, at 10 (July 29, 2008) ("although some of these attacks occurred before respondent [Reed Elsevier] acquired respondent Seisint, they continued for at least 9 months after the acquisition, during which time respondent Seisint was operating under the control of respondent [Reed Elsevier].").
8. See, e.g., Gramm-Leach-Bliley Act of 2000, 65 FR 31722, Title V, Subtitle A, § 502 (2000); SECURITY STANDARDS COUNCIL PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS, v. 3.0 (2013), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Joseph V. DeMarco is a partner at DeVore & DeMarco LLP. He previously served as an Assistant United States Attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property (CHIPs) program. Jeremy Apple is an Associate Attorney at DeVore & DeMarco LLP.

Looking for Past Issues?

Inside
Corporate Counsel Section Newsletter
<http://www.nysba.org/Inside>



How to Slay the Cyber Dragon: Lawyer-Supervised Privacy Programs

By Bruce H. Raymond

The time is now for corporations and the lawyers who serve them to take immediate, concrete steps to “up their game” on information security and privacy. As we approach the end of 2014, we are all on notice of the importance of this issue, yet almost no one is adequately addressing the risks associated with data breaches and their devastating economic consequences to businesses of all sizes.

The Problem

This has been the year of the so-called mega-breach with the first instance of a U.S breach (Target) costing in excess of a billion dollars.¹ According to a 2014 report from the office of the New York State Attorney General Scheiderman, data breaches cost entities doing business in New York \$1.37 billion in 2013 alone.² The report reveals that the number of reported data breaches has more than tripled between 2006 and 2013.³ Since 2006, 22 million personal records of New Yorkers have been exposed.⁴ “The New York Attorney General strongly suggests that all organizations that collect electronic information devise and implement a comprehensive data security plan.”⁵

The Fix

Large companies, such as Target and Home Depot, have tens of millions of dollars of insurance coverage, Chief Privacy Officers (CPOs), Chief Information Security Officers (CISOs) and ample data security resources deployed. Even with extensive resources, data breaches can and do happen to “the big guys,” so how are small and medium businesses to deal with such daunting risks?

The answer for small businesses is the same in principle as large companies: establish a lawyer-supervised privacy program.

The difference is that 95% of small and midsize businesses do not seek cyber liability insurance whatsoever⁶ and 87% have no written information-security plan in place.⁷ Further, small businesses are unlikely to have full-time data security executives such as a CPO or CISO; only 42% of companies with revenues under \$1 billion have an information security risk management team or committee.⁸

Privacy Programs Should Start with a Qualified Privacy Lawyer

As practitioners likely know, since 2005, New York law has required notification in the event of certain types of data breaches involving Personally Identifiable Information (PII) such as a name together with date of birth,

social security number, and financial accounts, or Personal Health Information (PHI).⁹ Non-compliant companies may face substantial fines and may have other onerous and costly remedies imposed such as mandatory audits and monitoring.¹⁰ New York-based companies that handle personally identifiable information of residents of other states (e.g., Massachusetts) may nonetheless be subject to regulatory or civil actions by those states as well. Forty-seven states have data breach notification laws with different requirements for reporting and serious financial consequences for breach.¹¹ Just the cost of sending out notice to customers can by itself be a costly and difficult endeavor. According to the Ponemon Institute, the cost in the United States for a data breach is \$195 per record.¹²

Federal and International Privacy Laws

In addition to state privacy laws, a complex web of Federal statutes may apply to information created or stored by New York companies. Unlike other countries, the United States privacy laws are organized by industry, or sector. Health care providers and their associates may be subject to HIPAA¹³/HiTech.¹⁴ Financial entities may be subject to Gramm-Leach-Bliley Act (GLB),¹⁵ The Fair Credit Reporting Act,¹⁶ Dodd-Frank Wall Street Reform and Consumer Protection Act¹⁷ and others. Educational institutions, transportation companies and telecommunications and marketing industries each have their own regulatory laws addressing privacy and data security issues.¹⁸ The above list is but a representative sample of the Federal laws which must be examined and navigated.

In today’s economy a good percentage of small businesses have dealings with businesses and consumers in other countries. International privacy laws may reach corporations dealing with other countries in North and South America, Europe, Asia and around the world. Even storing data, without more, may subject a company to regulation and impose requirements which, if breached, may subject New York companies to financial and other obligations.¹⁹

This summary of State, Federal and International laws impacting businesses illustrates that the privacy lawyer is the right tool for the job of identifying and interpreting the statutes, regulations, and judicial decisions which together operate to create potential risks and liabilities. There are a surprising number of non-lawyer consultants of various backgrounds offering privacy programs. Companies that use boilerplate privacy policies or rely on non-lawyer professionals to interpret and apply privacy laws are asking for trouble and missing important value.²⁰ An attorney’s communications of legal advice may qualify for protection from discovery under attorney-client privilege.²¹ Further,

attorney-directed investigations completed in anticipation of potential litigation or regulatory action may qualify for attorney work product privilege.²² If directed by an attorney, the work of other experts, such as forensic IT and data security experts, may be privileged.²³ In addition to getting the right advice, shielding sensitive legal advice from an opponent's discovery is a critical advantage that, in the event of litigation, could keep a case in the win column.

Tips on Finding Privacy Lawyers

Finding an appropriately qualified privacy attorney who is a good fit for your project may require some research. Companies with a large amount of multinational data transfers may be best served by a large law firm with offices in the countries with which the company has dealings. Companies with less complex business dealings may be better served by a boutique firm with appropriate experience and qualification. Another potential factor to consider when choosing counsel is whether the lawyer has specialized non-legal credentials such as Certified Information Privacy Professional (CIPP/US)²⁴ or Certified Information Systems Security Professional (CISSP).²⁵ Clients should inquire about a privacy lawyer's experience and focus. Some privacy lawyers only handle data breach response, others only deal with litigation; still others are more focused on transactional aspects of the law such as safe harbor and data transfer agreements.²⁶ Clients should also ask if the law firm handles privacy program work on an alternative or fixed-fee basis to control costs and help with budgeting the project.²⁷

Privacy lawyers are not the only professionals on the privacy team. Other professionals such as forensic IT data security experts, risk managers, insurance professionals, crisis management and public relations consultants are important components of the privacy program team.

People, Things and Processes

Once the lawyer or law firm is selected, the next step involves identifying the other professionals needed for a solid privacy program. First, the forensic IT/Data Security expert should be identified. This category of expert differs from a network administrator (a/k/a regular IT support) whose focus is more on making the information system work as distinguished from protecting data from hacking or unauthorized access. The forensic aspect addresses preservation of electronic evidence for use in court. Containing the breach is important to be sure, but it is not the only consideration.

The next member of the privacy team should be a cyber insurance expert. It is important to find a broker or agent who is well versed in the new insurance products available in this fluid and emerging market. So-called cyber liability insurance coverage does not have standard forms and there can be significant gaps or limits in the coverage.²⁸ If your current insurance professional is not knowledgeable regarding the details of cyber coverage,

it is wise to find a cyber specialist who does. Your cyber coverage must be examined along with CGL, D&O, E&O, Advertising and Media, IP, Professional Liability and other policies to identify any uninsured gaps or important limitations in coverage. Risk mitigation techniques or loss-spreading strategies must be deployed to manage risks associated with insurance gaps or limited coverage situations.

The outside experts need to work with senior management and internal stakeholders such as IT, HR and other department heads. The key internal stakeholders should form the Privacy and Information Security Committee, which is responsible for formulating privacy policy and implementing a response plan. Once the Privacy committee is established by management, the focus moves from people to things.

The "thing" aspect of a privacy program involves software and hardware designed to protect electronic information assets including, but not limited to, PII and PHI. Firewalls, antivirus, anti-malware, encryption, and physical security measures are examples of tangible protections and other barriers to limit unintended disclosure of information assets.

Privacy, Structures and Processes

In addition to people and things, perhaps the most important aspect of a successful privacy program is the process component. Privacy needs to become part of the core operating function of the company. A privacy program is not a one-and-done proposition; rather it needs to become a vital and evolving aspect of responsible management. To the extent a company is able to sustain reasonable and prudent protections for private information as technologies and threats change, the company will ultimately save money, keep the trust of its customers and benefit from a competitive advantage over the competition. In order to do business with "the big guys," increasingly small and medium businesses will have to certify as part of their contract that they are in compliance with various standards such as PCI, ISO and NIST.²⁹

Nuts and Bolts of a Privacy Program

What follows is an outline of some common issues and approaches that privacy programs address:

- Start your privacy program and development now and make it your goal to be in process by next quarter. If you are starting from scratch, it will take twelve months to get a base-line privacy program in place and functioning. Devote a modest amount of time each month to avoid biting off more than you can chew and allow for some flexibility so businesses can get done without overwhelming your team.
- Write your version of a policy statement to govern your program.

- Put one person in charge to “own” and be responsible for Privacy to management and give them authorization to act.
- Designate a chain of command so others are able to step forward if the senior privacy leader is not available.
- Complete a map of your IT infrastructure to include an inventory of every device with electronic memory from smart phones to servers.
- Map your data. Locate all electronic and paper copies of PII and PHI within the network. Don’t forget mobile devices, voicemail, scanners/copiers. Consolidate and encrypt private information and limit access to those who need it.
- Adopt Privacy by Design³⁰ principles or, as the Europeans might say, privacy by default.³¹ If you don’t need to use the data and you are not required to keep it, dispose of it in a reliable manner.
- Identify all outside persons or entities with either temporary or permanent access to your network including archive and software as a service (SaaS) providers.
- Develop vendor criteria and protocols and don’t approve vendors that cannot certify insurance and data security and privacy compliance.
- Require defense and indemnity contracts to cover data breach or accidental loss of PII.
- Create a written policy for B.Y.O.D. (use of employee owned devices) such as smart phones. These should be encrypted and companies should consider software which allows company-owned information to be reliably separated from personal communications.
- Determine if it is required or desirable from a business perspective to obtain certification on privacy compliance such as PCI, HIPAA, ISO and NIST.
- If a merger or acquisition is considered, establish a privacy compliance due diligence protocol to avoid issues in the deal. Make sure you are not buying another company’s data breach or privacy law violation.³²
- Establish, supervise, monitor and improve a training program for all categories of employees.
- Review HR policies and employee monitoring.
- Develop, train and test a data breach response program.

In conclusion, starting a data security and lawyer-supervised privacy program is not an option for some future time. If you start now, you can have an excellent program in place and protect your company by this time

next year. There are many resources to get started and make it happen.³³

Endnotes

1. Target’s breach began at the end of 2013 but the cost figures Target acknowledges is \$148 million in direct costs with some industry analysts estimating total costs to exceed \$1 billion. See TARGET CORP., CURRENT REPORT (FORM 8-K), EXHIBIT (99) (Aug. 5, 2014), available at http://www.sec.gov/Archives/edgar/data/27419/000110465914056760/a14-18360_1ex99.htm; THE FLY ON THE WALL, TARGET COULD BE FINED OVER \$1 BILLION FOR CARD BREACH, ANALYST SAYS (2014), available at <http://www.theflyonthewall.com/permalinks/entry.php/TGT;V;MA;AXPid1956406/TGT;V;MA;AXP-Target-could-be-fined-over-billion-for-card-breach-analyst-says>; citing DANIEL BINDER, NOTE TO INVESTORS (2014).
2. OFFICE OF N.Y.S. ATTORNEY GENERAL, INFORMATION EXPOSED: HISTORICAL EXAMINATION OF DATA BREACHES IN NEW YORK STATE (2014), available at http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf.
3. *Id.*
4. *Id.*
5. *Id.* at 2.
6. INSUREON, FEWER SMALL BUSINESSES BUYING CYBER LIABILITY INSURANCE SINCE TARGET’S BREACH (J2014), available at <http://www.prnewswire.com/news-releases/insureon-fewer-small-businesses-buying-cyber-liability-insurance-since-targets-breach-268097651.html>.
7. ADVISEN, CYBER EXPOSURES OF SMALL AND MIDSIZE BUSINESSES—A DIGITAL PANDEMIC 5 (2014), available at <http://www.advisenltd.com/wp-content/uploads/cyber-exposures-small-mid-size-businesses-white-paper-2014-10-14.pdf>.
8. ADVISEN & ZURICH, INFORMATION SECURITY AND CYBER LIABILITY RISK MANAGEMENT 7 (2014), available at <http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/information-security-cyber-liability-risk-management-white-paper-10-28-2014.pdf>.
9. N.Y. Gen. Bus. Law § 899-aa (CONSOL. 2014).
10. *Id.*
11. See NATIONAL CONFERENCE OF STATE LEGISLATURES, SECURITY BREACH NOTIFICATION LAWS (2014), available at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.
12. PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (2014), available at <http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF>.
13. 42 U.S.C. § 1320d-6 (1996).
14. 42 U.S.C. § 17921 (2009).
15. 15 U.S.C. §. 6801 (1999).
16. 15 U.S.C. § 1681 (1970).
17. DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT, 111 P.L. 203, Part 1 of 3, 124 Stat. 1376.
18. See, e.g., Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974); SAFETEA-LU, 49 U.S.C. § 31150 (2005); Telecommunications Act of 1996, 47 U.S.C. § 222 (1996); Telephone Consumer Protection Act, 47 U.S.C. § 227 (2010).
19. See, e.g., Graham Greenleaf, *Global Data Privacy Laws 2013: 99 Countries and Counting*, PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT (June 4, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305882. For example, companies dealing with the European Union will find themselves facing comprehensive privacy regulations, those dealing with Japan will face a sectoral model akin to the U.S., and those in Australia will work in a co-regulatory model.
20. See, e.g., Visa U.S.A., Inc. v. First Data Corp., 2004 U.S. Dist. LEXIS 17117 (N.D. Cal. Aug. 23, 2004).

21. N.Y. C.P.L.R. 4503 (CONSOL. 2002).
22. N.Y. C.P.L.R. 3101 (c) & (d)(2) (CONSOL. 2014).
23. See, e.g., 915 2nd Pub Inc. v. QBE Ins. Corp., 107 A.D.3d 601 (N.Y. App. Div. 1st Dep't. 2013).
24. See International Association of Privacy Professionals, *CIPP Certification*, IAPP, <https://privacyassociation.org/certify/cipp/> (last visited Oct. 30, 2014).
25. See CISSP®—Certified Information Systems Security Professional, (ISC)², <https://www.isc2.org/cissp/default.aspx> (last visited Oct. 30, 2014).
26. These terms refer to contracts under which U.S. Companies may certify compliance with the European Union or other countries privacy laws. See, e.g., *Welcome to the U.S.-EU Safe Harbor*, U.S. DEPT. OF COMMERCE, INT'L TRADE ADMIN (Apr. 11, 2012), http://www.export.gov/safeharbor/eu/eg_main_018365.asp.
27. My firm utilizes a monthly retainer model for our twelve-month privacy program.
28. See, e.g., Mark Silvestri, *Dealing with cyber risk: Closing the gaps in protection*, 28 J. HEALTHCARE & RISK MGMT 23 (Feb. 2009), available at https://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Dealingwithcyberrisk.pdf.
29. See, e.g., PCI Security Standards Council, *Requirements and Security Assessment Procedures v. 3.0* (2013), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf; Int'l Org. for Standardization, *ISO/IEC 27001:2013, Information Technology—Security Techniques—Information Security Management Systems—Requirements* (2013), available at <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>; Nat'l Inst. of Stds. & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (2014), available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.
30. See Ann Cavoukian, *Privacy by Design*, Ontario Information & Privacy Comm'n (2011), available at <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>.
31. See European Commission, *Proposed General Data Protection Regulation*, Art. 23 (2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
32. See, e.g., Edward Deibert, "Deciphering Due Diligence: Tackling the IT Issues That Can Cripple a Business Transaction" at Appendix A, ABA Annual Meeting (2010), available at <http://www.americanbar.org/content/dam/aba/publications/blt/2010/09/inside-buslaw-due-diligence-201009.authcheckdam.pdf>.
33. Many resources are available to companies that wish to learn more. See Peter Swire & Kenesa Ahmad, *Foundations of Information Privacy and Data Protection* (2012); Peter Swire & Kenesa Ahmad, *U.S. Private-Sector Privacy* (2012); Baker & McKenzie, *Global Privacy Handbook* (2013); Lucy Thomson, Ed., *Data Breach and Encryption Handbook* (2011); Harold Tipton, Ed., *Official (ISC)2® Guide to the ISSMP® CBK®* (2011); Steven Hernandez, Ed., *Official (ISC)2® Guide to the CISSP® CBK®* (3d Ed. 2013); Ronald Weikers, *Data Security and Privacy Law* (2011); Lisa Thomas, *Thomas on Data Breach: a Practical Guide to Handling Worldwide Data Breach Notifications* (2014). In addition to the above books, the IAPP websites also contains useful information. See <https://privacyassociation.org/>; <https://www.law360.com/privacy>; <http://www.advisenltd.com/networks/cyber-risk/>.

Bruce H. Raymond, J.D., CIPP/US is the current IAPP KnowledgeNet Chair for Connecticut and regularly represents clients throughout the country on privacy issues, data breach response and related litigation.

Your Foundation

The legal profession does so much to help so many.

By contributing knowledge, time, funding and a passion for justice; together we can have a meaningful impact in our communities across the state.


Your Gift Matters


If NYSBA members contributed just \$30 to The Foundation, over \$2 million would be available to expand legal community efforts.

This would help many more people in need and provide funding for law-related charitable and educational projects that are taking place in our neighborhoods across New York State.

When you make your gift to The New York Bar Foundation, you join with lawyers and others who share in our conviction that we must work together to bring equal access to justice to all New Yorkers.

Please give today. Call us at 518-487-5651 or give on-line at <http://www.tnybf.org/donation>





Lawyers caring. Lawyers sharing.
Around the corner. Around the state.

Social Media Evidence: To Authenticate or Not to Authenticate?

By Adam Cohen

In many cases, social media appears to have been accepted as evidence with nary a comment from the court about admissibility, nor even an objection. However, the number of cases where the authenticity of proffered social media has been challenged and rejected may be on the rise. The saga of *Griffin v. State of Maryland* (19 A.3d 415 (Md. 2011)) turns out to have been foreshadowing of the way the law is developing.

It clearly states the way circumstantial evidence has been used to argue for admissibility of social media, as well as why its authenticity may be open to question. In *Griffin*, an appellate court affirmed a conviction of second-degree murder and sentence of 30 years for murder based on finding no clear error by the trial court in admitting a printed page from MySpace into evidence. Defendant appealed the trial court's decision, arguing that the trial court erred by admitting into evidence the printed page from MySpace as allegedly belonging to the defendant's girlfriend since it was not properly authenticated and its prejudicial effect outweighed its probative value.¹

The appellate court concluded that the foundation of evidence provided—the officer's testimony that he believed the subject profile belonged to the girlfriend based on a photo of her with the defendant, her birth date, and references to the defendant noting his nickname—was sufficient to authenticate the printout. The court stated that there is no reason why social media profiles could not be circumstantially authenticated in the same manner as other forms of electronic communication, i.e., by their content and context.²

However, at the next stop on the appellate ladder the higher court rejected this determination, holding that the MySpace content was not properly authenticated.³ The court stated:

We agree with Griffin that the trial judge abused his discretion in admitting the MySpace evidence pursuant to Rule 5-901(b)(4), because the picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment. The potential for abuse and manipulation of a social networking

site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language.⁴

A number of recent cases involving Facebook evidence stake out these polar positions on social evidence. While a number of criminal cases in various states have accepted Facebook material as authentic evidence based on circumstantial evidence,⁵ other courts have viewed Facebook evidence as less trustworthy. These courts have also noted the possibility that the postings in question may have been fabricated.⁶

In the most recent precedential holding to date in this area, *U.S. v. Zhylytsou* (No. 13-803-cr (2nd Cir. 2014) (FindLaw)), the U.S. Court of Appeals for the Second Circuit vacated a conviction where evidence from a Skype account was admitted. Prosecutors sought to demonstrate that the defendant had emailed a forged birth certificate and introduced a printout of Skype account information showing a username matching the username of the email account used to send the forged certificate. The Second Circuit stated its position as follows:

Had the government sought to introduce, for instance, a flyer found on the street that contained Zhylytsou's Skype address and was purportedly written or authorized by him, the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhylytsou. Otherwise, how could the statements in the flyer be attributed to him?⁷

The Second Circuit makes a powerful point. Moreover, the Second Circuit Court of Appeals is a highly influential court. While some courts seem to be looking at social media evidence as similar to other evidence gathered from Internet (such as other website printouts), others have latched on to the ease with which social media accounts can be fabricated. Whether the Second Circuit's statement signals a new wave of skepticism regarding the authenticity of proffered social media will be closely watched.

Endnotes

1. 2010 Md. App. LEXIS 87 (Md. Ct. Spec. App. May 27, 2010).
2. *Id.* at *26.
3. 419 Md. 343, 357-58, 19 A.3d 415, 424 (2011).
4. *Id.*
5. See *Campbell v. State*, 382 S.W.3d 545 (Tex.Ct.App. 2012), *Simmons v. Commonwealth*, 2013 WL 674721 (Ken. 2013), *State v. Jones*, 319 P.3d 1020 (2014), *Parker v. State*, 85 A.2d 682, 688 (Del. 2014).
6. See, e.g., *U.S. v. Winters*, 530 F. Appx. 390, 395-96 (5th Cir. 2013) (“[The] photograph’s appearance on [defendant’s Facebook page] does not by itself establish that the owner of the page possessed or controlled the items pictured.”).
7. *U.S. v. Zhyltsou*, 13-803-cr. (2d Cir. 2014).

ANNUAL MEETING 2015



SAVE THE
DATE

January 26 – 31, 2015

New York Hilton Midtown
1335 Avenue of the Americas,
New York City

**Corporate Counsel Section/Business Law Section
Joint Program**

**The Business Survival Guide to Bitcoin; Privacy After the Breach;
What It Means to Your Clients and Their Customers**

Wednesday, January 28, 2015

For more information, go to www.nysba.org/am2015



Use and Defense of Data Subpoenas

By Charles Ross and Anne van Greevenbroek

Data privacy and security are paramount concerns in today's so called information age. Indeed, every time someone subscribes to any service such as a telephone, cable, and Internet package or a membership website, personal data is provided. In most instances companies that require personal information also have in place specific privacy policies regarding the release of personal information provided by customers. Many may assume that personal data is protected. However, privacy policies may give way to broader governmental interests as law enforcement agencies, prosecutors, and regulators have become increasingly more aggressive in their efforts to obtain data, including personal information, for ongoing investigations. Indeed, Verizon alone received almost 149,000 subpoena requests for electronic data this year, as well as orders, warrants and other emergency requests.¹

If regulators, prosecutors or law enforcement agencies want to obtain electronic data to further litigation or criminal investigations or charges and they do not have sufficient information to obtain a search warrant they must seek the data by way of subpoena. Subpoenas are a basic investigative tool which does not require a showing of probable cause to issue; where a grand jury is convened prosecutors have broader discretion to investigate. However, the main focus on the issuance of any subpoena is relevance, and the standards are set forth in Rule 17 of the Federal Rules of Criminal Procedure. Specifically, Rule 17(c) states that such things as books, records documents, and data may be the subject of a subpoena. However, Rule 17(c)(2) creates the possibility for a court to quash or modify subpoenas. A motion to quash a subpoena may be the first line of defense in dealing with an investigation, but there must be some basis to claim a subpoena should be quashed. Lack of relevance, privilege, over breadth, and lack of specificity are but a few grounds often cited by counsel moving to quash a subpoena.

There are two recent cases where a warrant or subpoena was served to collect data from companies about individuals. The subpoena to collect data becomes more critical because data can be stored anywhere in the world now. Also, users are located all around the world, but to what extent is the data of your client protected? Does a subpoena or warrant reach foreign countries when the data is stored abroad, even though the recipient of the subpoena is an American company? The instant globalization provided by the Internet, and the proliferation of data and new communication systems have expanded exponentially. Two recent cases highlight a number of these issues.

Microsoft Corporation

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation, 13-MAG-2814; M9-150, involved a scenario in which Microsoft Corporation received a search warrant on December 4, 2013 to hand over personal information. The warrant that issued demanded digital information, which is stored outside the U.S.,² associated with a member of the public's email account, and included the member's name, address, credit card details and contents of all messages. When a user signs up with Microsoft Corporation, each is assigned to datacenters in more than 100 facilities spread over 40 countries according to their proximity. The court in *Microsoft* observed that Rule 41 (dealing with search and seizure and warrant requirements) of the Federal Rules of Criminal Procedure is silent as to whether it has extraterritorial effect. Therefore, Microsoft Corporation argued (1) that the warrant would require an extraterritorial search and seizure of data stored in its datacenter positioned in Ireland and; (2) that the Government cannot execute the search and seizure in Ireland, because Rule 41 provides no authorization for extraterritorial application. Microsoft also argued that the USA Patriot Act amended the Stored Communication Act (SCA) to allow judges to issue a subpoena for other districts, and therefore it authorizes a nationwide service and not worldwide service.

The Stored Communications Act is a part of the Electronic Communications Privacy Act of 1986 (ECPA).³ These provisions seek to protect the online privacy of individuals and entities on the internet. It applies to data which is stored electronically, to email, and to telephone conversations. The SCA protects the privacy of records of a subscriber held by the service provider and files stored by service providers. Thus, service of a subpoena will clash with the interests protected under the ECPA and SCA.

While Microsoft Corporation also pointed out to the court that there was an amendment in 1990 to Rule 41 to permit issuance of warrants to search property outside the U.S., the Supreme Court rejected it. Hence, Microsoft Corporation filed a motion to vacate the search warrant on the grounds that Rule 41 authorized no foreign execution of search warrants.

Microsoft Corporation's motion to vacate the search warrant was denied by the magistrate judge. The court found that if a warrant was issued under the SCA, the warrants are "hybrids"—part warrant and part subpoena. Under the SCA a warrant is obtained through a probable cause application and determination by a judge, but it is executed like a subpoena. The magistrate judge in *Microsoft* opined that the actual search does not occur until the

data is reviewed by the law enforcement agencies in the U.S., which means that there is no extraterritorial search.

Microsoft Corporation stated that the ruling vitiated the Fourth Amendment to the United States Constitution, weakened security of data and information for the entire world, and allows global reach in light of a gutted Fourth Amendment.

A number of amicus briefs were filed in support of Microsoft's position. Indeed, the Electronic Frontier Foundation, Verizon, Apple, Cisco, and AT&T all filed briefs in support of protecting the privacy of the data at issue.

Even though the judge denied Microsoft Corporation's motion to vacate and said that Microsoft Corporation had to hand over the overseas-held emails, Microsoft Corporation will continue to withhold the information as it waits through the appeals process. Until there is a final decision regarding this process, an open issue remains as to whether or not data held overseas is protected from subpoenas and warrants.

AirBnb Inc.

In *AirBnb, Inc. v. Eric T. Schneiderman, Attorney Gen. of New York*, 5393-13,⁴ the company marketed an online platform for individuals to rent their apartments to tourists or other third party visitors. The New York Attorney General (NYAG) issued a subpoena dated October 2013 and demanded that AirBnb produce an excel spreadsheet which identified personal information about all the homeowner "landlords" who rent accommodations in New York. The NYAG's office also subpoenaed documents related to all tax-based communications AirBnb had with customers who rented out their apartments or homes.

AirBnb claimed (1) that the subpoena had no factual basis, and (2) was overbroad and unduly burdensome. Thus AirBnb moved to quash the subpoena. In addition, AirBnb also argued that there was no actual basis for the subpoena and that the process was an unfounded fishing expedition. Moreover, AirBnb claimed that the NYAG's investigation was based upon laws that are unconstitutionally vague and the subpoena was seeking confidential and private information from AirBnb's users.

The NYAG's office responded that the subpoena was focused only on hosts who the NYAG's office believed were violating the law. The subpoena was limited to about 15,000 people instead of the information of all the people in the State of New York.

Judge Gerald W. Connolly ruled that the NYAG's data subpoena was overly broad, because "the subpoena was not limited to New York City hosts or those who reside in cities, towns or villages that have adopted the Multiple Dwelling Law."⁵ The judge rejected all other arguments.

Yet again there was serious amicus involvement in this matter as well. Amicus briefs were filed by The Electronic Frontier Foundation (EFF) and the Center for Democracy & Technology. Both argued that the NYAG had not articulated a basis to believe AirBnb was even under investigation and that the demand itself was overbroad.

Considerations When Issuing a Data Subpoena

When issuing a data subpoena there are some practical things you have to consider while doing it. There are some guidelines set in *U.S. v. Nixon*, 418 U.S. 683, about which documents fall within "any documents" from Rule 17(c) and with which requirements the data subpoena must comply. The Supreme Court decided in *Nixon* (1) that the serving party has to show in the subpoena that the documents are relevant and evidentiary. It also stated that (2) the documents are not otherwise procurable reasonably in advance of trial by exercise of due diligence.

The subpoenaing party must demonstrate that the production of the documents is necessary for a proper preparation for trial and that a failure to produce the data would lead to unreasonable delay of trial. Finally, the party issuing the subpoena must show good faith and cannot engage in a "fishing expedition."

In *Nixon* a motion to quash the subpoena was filed, but the District Court denied it and the Supreme Court upheld the denial of the motion because it found that the subpoena complied with all the requirements under Rule 17(c).

Considerations in Effectively Defending Against a Data Subpoena

When your client receives a data subpoena it is necessary to review the electronic documents and files to decide whether or not your client has to produce them. Here is an overview of the issues to consider when your client is served with a data subpoena.

Was service improper? While this is not a particularly effective argument as the requesting authority will probably simply affect proper service, it should be considered.

Is the data sought confidential material? For example documents held by doctors or lawyers may contain private and protected information about their clients or patients.

Is the information requested in an overbroad manner? Will the information be impossible to gather without more specificity, narrowing, or accepting a representative sample? If so, a motion to quash should be considered, or at the very least specificity should be sought.

Is the request so broad and irrelevant as to constitute a fishing expedition? If so a motion to quash should be filed. Vagueness and relevance are also issues to analyze. In addition, when producing data in response to a

subpoena or warrant the “act-of-production-doctrine” should be closely considered. A designated document custodian should always be appointed. Clerks, secretaries, personal assistants are all fine choices. Thus, if a regulator or prosecutor seeks to introduce data, the custodian can authenticate it. Directors, officers, subjects and targets should never gather documents for production as their testimony can be compelled as a waiver of the act of production privilege.

Conclusion

It is obvious in our brave new world of globalized data that regulators and prosecutors will continue to seek to expand the reach of their ability to seek data. Using the strategies set forth in this article can be a start to defending against this broad attack on privacy and assist in the use of data subpoenas as a means of discovery.

Endnotes

1. <http://time.com/2970139/verizon-customer-data-requests/>.
2. The Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation, Cas. Nos. 13-MAG-2814; M9-150.
3. Pub. L. 99-508, 100 Stat. 1848 (October 21, 1986).
4. Which is held in the State of New York Supreme Court, County of Albany.
5. Decision and Order, index no. 5393-13, p. 8.

Chuck Ross has successfully represented a wide variety of individuals and companies in both criminal and administrative matters—from stockbrokers, investment advisers, hedge fund managers, and compliance officers to noted entertainers and athletes. Chuck is a member of the National Association of Criminal

Defense Lawyers, the New York Council of Defense Lawyers, and the Federal Bar Council. He serves as vice chair of the Judiciary Committee of the New York City Bar Association, and frequently lectures on topics involving white collar defense and criminal trial skills and strategy. He has consulted on criminal justice issues for the *Wall Street Journal*, the *New York Times*, and CNBC and Court TV. Prior to founding Charles A. Ross & Associates, he was chair of the White Collar Criminal Defense Group at Herrick, Feinstein, and a name partner at the boutique criminal defense firm Brafman & Ross (now Brafman & Associates). As Assistant Federal Public Defender in the Southern District office of the Legal Aid Society’s Federal Unit from 1988 to 1991, he conducted numerous jury trials to verdict. Before that, he was a trial attorney for the Criminal Defense Division of Legal Aid in the South Bronx. He is a cum laude graduate of New York Law School.

Anne van Greevenbroek has been an intern at Charles A. Ross & Associates. She is a law student in the Netherlands. She worked at the firm from September 2014 and will stay through part of January 2015. She received her Bachelor in Law in 2013 at the Erasmus University Rotterdam, the Netherlands. In addition she is currently completing two Master’s degrees at the Erasmus University Rotterdam; one in Criminal Law. After graduation she plans to start work as a criminal defense attorney in the Netherlands. Besides her study, Anne was for a year a fulltime member of the board of a student association in Rotterdam and was Secretary of the board of Foundation BeSt, which organizes events for the city of Rotterdam and disabled people. She also did an internship for eight months at the District Attorney’s Office of Rotterdam, the Netherlands.

Request for Articles



If you have written an article and would like to have it considered for publication in *Inside*, please send it to either of its editors:

Jessica D. Thaler
410 Benedict Ave.
Tarrytown, NY 10591
jthaleresq@gmail.com

Matthew Bobrow
375 South End Avenue
New York, NY 10280
Matthew.bobrow@law.nyls.edu

Articles should be submitted in electronic document format (pdfs are NOT acceptable), and include biographical information.

www.nysba.org/Inside

Damned if You Don't: Addressing Law Firm E-Discovery and Data Security Challenges

By John J. Jablonski

To the uninitiated, e-discovery is often viewed as a necessary nuisance only the litigation lawyers need to deal with. Firm management and non-litigation lawyers know it exists, and they are aware of how vast and complex it can be, but they largely stay away from the nuts and bolts of the process.

That model isn't going to cut it anymore. Technology refuses to slow down, and data breaches are on the rise. If law firms do not keep pace and appreciate, from the top down, the importance of data security and e-discovery, they may be sailing into a perfect storm for catastrophic security breaches involving the e-discovery process.

It wasn't long ago that e-discovery was limited to large, complex litigation. But we now live in a digital world where nearly all discoverable information is created and stored electronically, so it permeates all litigation. Yet many lawyers (and judges) continue to demonstrate a surprising lack of knowledge about technology and the e-discovery process. Price pressure on e-discovery is stronger than ever as well, thanks to the economic downturn and the resulting increase in clients refusing to foot exorbitant bills for e-discovery. Because of that, many firms have cut back on spending for the technology and people needed to support a robust e-discovery process.

On top of this economic pressure comes heightened scrutiny from clients regarding law firm data security, including during e-discovery. In 2011, the FBI held a meeting of 200 law firms in New York to warn them of specific attacks targeting law firms,¹ highlighting how real the threat has become for them. In 2013, headlines were filled with large retail data breaches. Cyber security has risen to the number one concern of board members of private companies and large publicly traded companies.²

All this leaves law firms in a bit of a catch-22. In a very competitive legal market, investing resources in data security may not win praise from a client (or cost conscious partners), but failing to address security vulnerability is a sure-fire way to lose a client. "When people say, '[w]e won't pay you money because your security stinks,' that carries weight."³ Data security in the e-discovery process, like all other law firm data security concerns, must be addressed.

Data Security Challenges During E-Discovery

Many data security "pinch points" exist during the e-discovery business process. While there is some overlap with overall firm security, several potential vulnerabilities are unique to e-discovery.

Law firm data security e-discovery challenges are best categorized into two broad categories: inward-facing and outward-facing challenges. Inward-facing challenges are data security issues related to the firm itself, should it ever be involved in litigation—essentially the same issues that any business needs to be aware of in today's technology-driven world. Outward-facing challenges involve the data security issues faced by the law firm as it works to protect client data during the e-discovery process, including adhering to each client's specific data security requirements.

Inward-Facing Data Security—Law Firm Challenges Related to Data Security

Inward-facing data security challenges are those faced by the law firm itself when up against governmental or civil investigation or litigation (for example, the law firm is facing claims involving malpractice, contract disputes or non-compete agreements, to name just a few).

To meet these challenges, law firms should follow the same advice they should give to any of their business clients and address: 1) establish policies related to data security and information management; 2) create physical and technical controls related to security; 3) provide education and training related to security, information management and e-discovery; 4) identify trigger events and issue litigation holds when litigation or government investigation is reasonably anticipated; 5) set up preservation protocols related to securing, collecting and storing electronically stored information ("ESI") in a defensible manner; and 6) consider data privacy challenges based on the geographic reach of the law firm and the nature of the information stored at the firm.

Data Security and Information Management Policies and Procedures

Establishing good information governance principles (where information is stored and how) as well as the data security infrastructure (physical and technical controls) to protect data are essential for law firms. Law firms need to have in place policies and procedures governing the creation, storage and dissemination of information within and outside the firm. Policies need to be taught and enforced. Information and data governance policies and procedures establish the rules that employees of the firm follow. They serve as a reference for compliance. More importantly they are rules for addressing unacceptable practices jeopardizing firm security. The belief that employees understand the need to protect client data is insufficient protection. Employees need guidance. Even

the best-intentioned employees—without policies and training—can subject the firm to unacceptable security risks.

Physical and Technical Data Security Controls

Physical controls relate to building access to systems and computers to prevent theft and tampering. Some examples are locks, signs warning of restricted access, surveillance cameras, alarms, key access using identification badges for employees and private security service or patrols.

Technical controls involve the use of firewalls, encryption and simple protections such as strong password protection and terminal locks after a few minutes of inaction (such as when an employee walks away from a desk). Technical controls can include unique user identification methods, automatic logoff, encryption, authentication, and integrity controls.

Another common way data is breached at a law firm is through lost laptops and devices. Employees need to be trained to report such breaches immediately. Firms need to manage laptops, storage media (like thumb drives or USB hard drives) and mobile devices with technical controls (such as encryption and strong password protections) to prevent sensitive client data falling into the hands of anyone stumbling onto a lost device in a cab or at the coffee shop.

In the event mobile devices contain sensitive client data, law firms need to have the ability to wipe the device remotely in the event that the device is lost or stolen.

Data Security Awareness, Education and Training

Raising employee awareness through education, training and an internal data security awareness campaign is critical to teaching law firm employees about data security. While much attention is focused on threats posed by sophisticated hackers the vast majority of data breaches are aimed at the weakest link in the data security chain: employees. A hacker can easily send a phishing email containing malware thousands of times. The hacker needs just one employee at a law firm to click on the link or attachment to download malware into your system to gain access.

Some criminal tactics are as simple as calling a law firm and impersonating IT support (sometimes called the help desk) to obtain the login and password credentials of an employee simply by asking them. Training employees to challenge visitors without nametags is essential in larger firms where employees are not fully familiar with the names and faces of their colleagues. Physical access controls also are necessary to prevent someone from walking into the firm and sitting at a terminal. In one reported incident, a hacker was able to learn login and password information from bank employees by observing employees through a window.

Litigation Holds

Litigation hold policies and procedures should be established as part of information governance. Law firm employees should be trained on preservation and their role in the litigation hold process. Employees should understand potential trigger events and how to report them to the general counsel's office or firm management. Whenever litigation is threatened or initiated against the law firm steps must be taken to ensure that ESI is being preserved. Auto-delete settings on email, networks and other systems that automatically delete files as part of routine data storage protocols should be turned off for custodians subject to a litigation hold.

Firms also need the ability to preserve data in cloud or vendor data storage areas that courts may deem within the possession, custody or control of the law firm (based on a factual analysis of the practices of the firm and its employees—including contractual relationships with vendors). These locations include any third party applications controlled by employees used to store work related data, such as Dropbox,TM Box.netTM and Google DriveTM (to name a few "cloud" storage locations). Law firms must also devise methods of preservation and collection of data stored on mobile devices such as iPhones,TM AndroidTM devices and tablets.

As will be discussed below, ESI must not be altered during the preservation or collection process. If a firm lacks the internal expertise to properly preserve and collect ESI, it should secure the services of an outside vendor.

E-Discovery Procedures

Law firms are not immune to their own e-discovery headaches when sued, given the large volume of data created, stored and disseminated by law firms among staff, lawyers, courts, opposing counsel and clients. Law firms must be aware of the e-discovery pinch points discussed below and take steps to ensure proper data security protocols are followed during e-discovery involving law firm data. It is essential that law firms do their best to proactively address security during e-discovery involving their own data.

Privacy

Law firms must be aware of the data privacy laws in the jurisdictions of their offices. Care must be taken to abide by applicable privacy laws when collecting data from countries outside the United States—which have strict laws prohibiting or limiting a firm's access to employee files (even with the employees consent).⁴

Law firms must also be aware of the privacy laws in the states where they have offices.⁵ Firms spend a lot of time focused on client concerns, but they must also think of risks to their own data related to employees, such as names, address and social security numbers sufficient to meet the definition of personally identifiable information ("PII") in most states privacy laws. Once employee data is

accessed, a law firm may have a duty to report the breach and notify affected employees. Also, firms need to think of all areas where PII may be stored, such as firm administered credit cards, reimbursement forms, employment files, background checks and retirement account information. In most states, loss of employee PII triggers mandatory notification to employees and the need to report data breach incidents to state agencies.⁶

the firm, at a vendor or in the cloud); and 3) disclosure of client data to adversaries.

Protecting Client Data During Preservation and Collection

Protection of client data while gathering ESI (known in the e-discovery world as “collection”) has two main components. First, data must be collected in a defensible way in accordance with case law applicable to the juris-

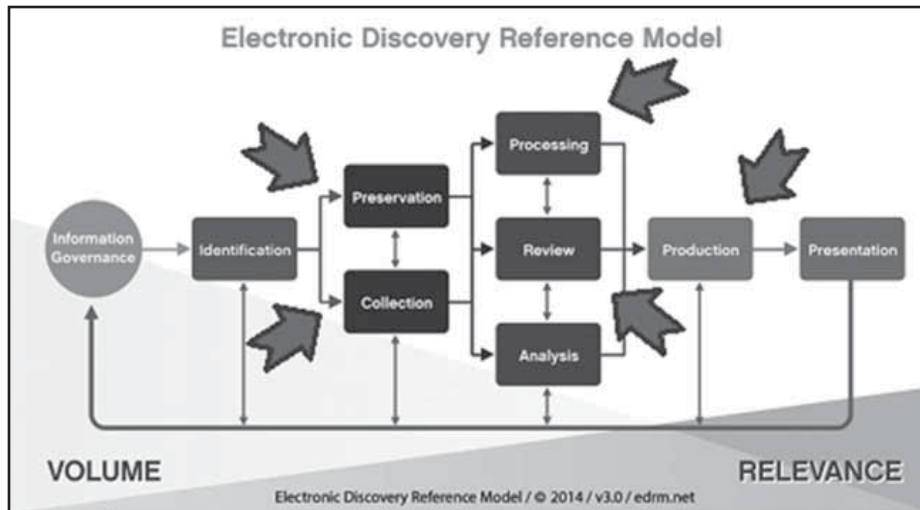
diction and the dictates of any particular case (including protocols agreed to with an adversary or required by the court related to collection and production). This means having people in place that are knowledgeable; having access to technology tools sufficient to protect the integrity of client data; and having processes in place to defend the method of collection.

The main goals during collection are to ensure that the metadata associated with files is not destroyed and a defensible chain of custody is maintained. Metadata is the information stored with a file about its contents, such as storage location, author, date of creation, subject and file type, to name a few (e-discovery

practitioners like to describe metadata as “data about data”). Metadata is often not very relevant to the parties (it’s the content of the electronic document that is relevant). Metadata, however, is a key component of the e-discovery process. ESI is often disclosed with an access to a small number of fields of metadata to help parties catalog and analyze ESI. In the vast majority of e-discovery disclosures, metadata related to the custodian, author, date, subject and other basic information about the files being disclosed is exchanged as a matter of course. Slip-ups in this area can result in a costly collection “do-over” or sanctions.

Protecting the integrity of the data is necessary to defending the process used to collect data. When an e-discovery fight ensues, often opposing counsel challenges every aspect of the chain of custody of the data. The goal of a party seeking to establish spoliation is to raise doubts about the integrity of the process and collection can be fertile ground. Loading files into Dropbox™ to facilitate collection, for example, may not carry the burden of a defensible e-discovery process. Other blunders like the loss of unencrypted data by the overnight delivery carrier could wreak havoc on the ability to defend the e-discovery process. As concerns over data security rise, so too will attacks by an adversary on the security protocols used during e-discovery.

Demonstrating adequate security controls is a key part of defending the e-discovery process. Attorneys may need to show that the method of collection did not alter metadata. This may include demonstrating that transfer



E-Discovery Data Security Pinch Points⁷

Outward-Facing Data Security—Law Firm Challenges Related to Client Concerns

Outward-facing data security challenges faced by law firms are based on client data security needs. Although our focus is on e-discovery issues, client data security concerns cut across all legal services rendered by a law firm. Clients are concerned about their data in a way never before seen. High-profile data breaches and the exorbitant costs of responding to a data breach have put companies on alert with all of their vendors and business partners, including law firms.

Some firms have faced security audits, and some clients are now requiring law firms to execute data security agreements. These agreements shift liability to law firms in the event of a data breach involving client data and require the firm to agree that is adhering to client specific data security protocols. The American Bar Association has adopted proposed changes to Rule 1.1 of the ABA Model Rules of Professional Conduct, requiring lawyers to keep pace with technology changes.⁸ Some commentators have suggested that a breach in data security could result in malpractice claims. This should come as no surprise as problems related to e-discovery have resulted in some high-profile legal disputes between clients and their former firms.⁹

Outward-facing data security concerns track the e-discovery life cycle. These concerns relate to protecting client data during: 1) preservation and collection of client data; 2) review, processing and analysis of client data (at

of data from client to law firm was handled using secure methods of transfer. In other words, counsel may need to show that access was limited to a small group of individuals and security measures prevented data from being altered or accessed.

In a recent Verizon report on data security, losing data (through forgotten laptops, thumb drives and mobile devices) was ranked as one of the largest sources of data breach for organizations.¹⁰ Sending an unencrypted thumb drive via overnight delivery is like sending boxes of documents on the back of a pickup truck. If the boxes are lost, it is not difficult to imagine them being found and sensitive information being published online. Digitally stored data is no different. If the data can be accessed it can be seen, read and posted online.

Privacy is another big data security concern. Data coming from outside the United States is subject to other countries' strict data privacy laws. In the United States, data containing personally identifiable information—usually defined as names associated with social security numbers—is subject to data breach laws now existing in 48 states. Data containing patient medical records is subject to HIPAA/HiTECH data protection requirements. Recent expansion of these laws subjects law firms to fines if Protected Health Information is accessed by unauthorized personnel or inadvertently disclosed.

Protecting client confidences is yet another big concern. The loss of a hard drive containing client data can be sufficient to demonstrate that care was not taken to protect the privileged nature of the attorney-client communications pursuant to applicable privilege law. A security mishap by a law firm could destroy a client's ability to protect privileged documents from disclosure.¹¹

Tips for protecting data security include:

Explaining security risks to your client—an open line of communication about data security, including client expectations and requirements is key to applying adequate data security controls during e-discovery.

Protecting the firm using e-discovery specific agreements and retainer agreements—law firms should address data security in their contractual agreements with e-discovery vendors and within client retainers.

Specific liability waivers during e-discovery—if a client resists adequate security controls law firms should reach an agreement (and where possible a written waiver of liability) should a client insist on transfer of data in a less than secure manner.

Complying with client data security requirements—compliance with client data security requirements goes beyond agreeing in writing. Law firm relationship managers need to understand client data security requirements and coordinate with a chief security officer or outside consultant to ensure compliance. Some

clients have started auditing law firms for compliance with data security requirements and it is only a matter of time when even the smallest law firms face data security audits from clients concerned about data security.

Conduct internal data security audits—knowing the firm's vulnerabilities long *before* a client chooses to audit the law firm will allow time for the law firm to address any weaknesses in its policies, procedures, e-discovery protocols and physical or technical controls.

Protecting Client Data During Processing, Review and Analysis

Once collected from the client the next security pinch point in the e-discovery process is the processing, review and analysis of the data prior to it being disclosed to an adversary. The storage of data must be secure, whether at the law firm or the vendor. A defensible protocol for storage, processing, review and analysis is critical for protecting the security of the data, client confidences and protecting the attorney-client privilege.

Tips for protecting data security include:

Ensuring data is stored in a secure server location—whether at the firm or at a vendor, review internal or vendor security protocols meet or exceed your client's requirements.

Limiting access to the data to need to know team members—use, when possible, technical controls to limit access to e-discovery data to team members. When stored at a vendor, access should be authenticated and logged to protect against unauthorized access. Passwords should be assigned to individuals and not shared across the team. Passwords should be changed frequently.

When using contract attorneys—it is best to limit the team to vetted and trusted contract attorneys. If at all possible, downloading of data from the review tool should be prohibited for contract attorneys. If sensitive privileged documents are in the data set, consider using on-site review, which cannot be accessed remotely. If highly sensitive documents exist within the data set, consider storage and review on a closed network with no other network or internet links whatsoever. This will limit access to the terminals connected to the data set.

Data destruction—plan for the end-of-life destruction of the data set upfront in accordance with client guidelines. Have a written protocol in place for the method of destruction. Copies of data should be limited as much as possible and all copies should be destroyed as soon as they are no longer needed. Be sure to avoid destruction of all or a part of a data set that may be subject to other litigation holds. Be sure to obtain a certificate of destruction from a vendor or provide a certificate of destruction to the firm's client if end-of-life the law firm performs destruction.

Plan for “operator error”—have a plan in place for responding to potential security incidents during the storage, review and analysis process. Be sure to give team members instructions related to some typical scenarios, such as losing their laptop or a thumb drive containing data related to the project. Hotlines for reporting lost or stolen devices are helpful.

Protecting client information at a vendor—be sure that data security is raised as a concern during the vendor vetting process, including a review of the vendor’s data security protocols. Have a frank discussion about data security with the e-discovery vendor. Client and firm data security requirements should be in writing and made part of the statement of work or as an addendum to the master services agreement or terms and conditions of the law firm’s contract with the vendor.

Protecting Client Data During Disclosure

The last pinch point in protecting data security during e-discovery may be the most difficult to control; i.e., the security of ESI once it is produced outside the law firm. Whether dealing with the government or an adversary, data security may not seem like an option. Discussing data security with an adversary is essential, when dealing with highly sensitive client documents during e-discovery. When possible, data security should be addressed in written agreements, protocols or through a court order.

Clawback agreements agreed to among counsel (governing how parties will deal with inadvertently disclosed ESI) should address data security. If at all possible a clawback agreement or e-discovery protocol should address minimum data security requirements among adversaries. Consequences of a data breach by your adversary should be addressed. Access to information disclosed during the e-discovery process should be limited by the agreement. Lastly, e-discovery protocols among adversaries should also provide for the return or destruction of all data disclosed to an adversary during the e-discovery process. This includes, when possible, ensuring an adversary does not retain backup copies of disclosed ESI in its disaster recovery system.

The Changing Data Security Landscape

Now, more than ever, the spotlight of data security is being shined on clients as a result of recent high profile data security incidents. In turn, clients are shining the data security light on their law firms. The e-discovery process is an integral part of the attorney-client relationship and gaps in security can have costly ramifications related to the loss of the attorney-client privilege, escalating e-discovery costs, sanctions and the erosion of client trust in its outside law firm. Law firms can maintain client trust by addressing overall firm data security and focusing specific attention on data security pinch points during e-discovery.

Endnotes

1. Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG (Jan. 31, 2012, 4:37 PM), <http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html>.
2. MICHAEL BREIT & STEVEN KREIT, CONCERNS ABOUT RISKS CONFRONTING BOARDS, EISENAMPER LLP (2014), available at http://www.eisneramper.com/uploadedFiles/Resource_Center/Articles/Articles/EisnerAmper-Concerns-Risks-Survey-2014.pdf?id=6442451343.
3. Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, N.Y. Times, Mar. 26, 2014.
4. NEIL ROBINSON, ORLA LYNSEY, & MICHAEL GREENBERG, E-DISCOVERY AND LEGAL FRAMEWORKS GOVERNING PRIVACY AND DATA PROTECTION IN EUROPEAN COUNTRIES (Rand Europe ed. 2010), available at <http://www.ftitechnology.com/doc/white-papers/whitepaper-rand-implications-part-one-2010.pdf>.
5. JOHN JABLONSKI & D. GERBER, COMPENDIUM OF U.S. DATA BREACH AND PRIVACY LAWS (Goldberg Segalla LLP ed. 2014).
6. *Id.*
7. The author used red arrows on the “E-Discovery Reference Model” to identify data security “pinch points.” See *Electronic Discovery Reference Model (EDRM)*, EDRM, <http://www.edrm.net/resources/guides/edrm-framework-guides> (last visited Oct. 28, 2014).
8. “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant **technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.” ABA RESOLUTION 105(A) REVISED (adopted Aug. 6, 2012) (emphasis added) (proposing additional comment to Model Rule 1.1).
9. For example, in 2011, a law firm was sued following a botched e-discovery project resulting in 4,000 privileged documents being disclosed. See *Complaint, J-M Manufacturing Co. v. McDermott Will & Emery*, BC462832 (Cal. Super. Ct. June 2, 2011), http://amlawdaily.typepad.com/06062011jm_mcdermott.pdf (last visited Oct. 28, 2014); see also *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 638108 (S.D. Cal. Mar. 5, 2008) (referring counsel to state bar association for failure to disclose relevant electronically stored information).
10. *2014 Data Breach Investigation Report*, VERIZON (2014), available at <http://www.verizonenterprise.com/DBIR/2014>.
11. Beth Winegarner, *Big Law Firms Are Most Vulnerable To Hackers: ABA Panel*, LAW 360 (Aug. 9, 2013, 9:47 PM), <http://www.law360.com/articles/464016/big-law-firms-are-most-vulnerable-to-hackers-aba-panel>.

John J. Jablonski is a partner in Goldberg Segalla’s New York office, where he serves as chair of the firm’s E-Discovery Practice Group and co-chair of its Cyber Risk and Social Media Practice Group. He holds leadership roles in a number of national organizations in these areas, including the chair of DRI’s E-Discovery Committee and Program Chair of DRI’s Data Breach and Privacy Law Seminar. He is a frequent presenter and author on data security, data breach litigation, electronic discovery, electronic evidence investigation and preservation, best practices for data security, privacy and preservation. He serves as his firm’s Chief Information Security Officer as well as leading the technology team. In 2013, he received the Alfred W. Cortese, Jr. Award from Lawyers for Civil Justice in recognition for his expertise in electronic discovery.



THE NATIONAL ACADEMY OF DISTINGUISHED NEUTRALS

NEW YORK CHAPTER

www.NYMEDIATORS.ORG

NAME	BASED IN	PHONE	CALENDAR	NAME	BASED IN	PHONE	CALENDAR
David J. Abeshouse	Uniondale	(516) 229-2360	<input checked="" type="checkbox"/>	Hon. Allen Hurkin-Torres	New York	(212) 607-2785	
Prof. Harold I. Abramson	Central Islip	(631) 761-7110		Irwin Kahn	New York	(212) 227-8075	
Simeon H. Baum	New York	(212) 355-6527	<input checked="" type="checkbox"/>	Jean Kalicki	New York	(202) 942-6155	
Leona Beane	New York	(212) 608-0919	<input checked="" type="checkbox"/>	Harold A. Kurland	Rochester	(585) 454-0717	<input checked="" type="checkbox"/>
Howard N. Beldock	New York	(212) 967-6799	<input checked="" type="checkbox"/>	Lela Porter Love	New York	(212) 790-0365	<input checked="" type="checkbox"/>
David M. Brodsky	Scarsdale	(212) 906-1628	<input checked="" type="checkbox"/>	Richard Lutringer	New York	(917) 830-7966	<input checked="" type="checkbox"/>
William J.T. Brown	New York	(212) 989-2475		Robert E. Margulies	New York	(201) 207-6256	<input checked="" type="checkbox"/>
Mark J. Bunim	New York	212-683-0083		Michael Menard	Hamburg	(716) 649-4053	<input checked="" type="checkbox"/>
Steven Certilman	New York	(212) 956-3425	<input checked="" type="checkbox"/>	Peter Michaelson	New York	(212) 535-0010	
Douglas S. Coppola	Buffalo	(716) 852-4100	<input checked="" type="checkbox"/>	Charles J. Moxley Jr	New York	(212) 329-8553	<input checked="" type="checkbox"/>
Gail R. Davis	New York	(646) 246-8043		Shelley Rossoff Olsen	New York	(212) 607-2710	
Jacquelin F. Drucker	New York	(212) 688-3819	<input checked="" type="checkbox"/>	Lawrence W. Pollack	New York	(212) 607-2792	
Howard S. Eilen	Uniondale	(516) 222-0888		Ruth D. Raisfeld	White Plains	(914) 722-6006	<input checked="" type="checkbox"/>
Eugene I. Farber	White Plains	(914) 761-9400		Margaret L. Shaw	New York	(212) 607-2761	
Alfred Feliu	New York	(212) 763-6802	<input checked="" type="checkbox"/>	Vivien B. Shelanski	New York	(212) 607-2707	
Ronnie Bernon Gallina	New York	(212) 607-2754		Richard H. Silberberg	New York	(212) 415-9231	<input checked="" type="checkbox"/>
Barry H. Garfinkel	New York	(212) 735-2500	<input checked="" type="checkbox"/>	David C. Singer	New York	(212) 415-9262	<input checked="" type="checkbox"/>
David Geronemus	New York	(212) 607-2787		Steven Skulnik	New York	(646) 231-3457	<input checked="" type="checkbox"/>
Eugene S. Ginsberg	Garden City	(516) 746-9307	<input checked="" type="checkbox"/>	Norman Solovay	New York	(646) 278-4295	<input checked="" type="checkbox"/>
Krista Gottlieb	Buffalo	(716)-218-2188	<input checked="" type="checkbox"/>	Hon. Joseph P. Spinola	New York	(212) 967-6799	<input checked="" type="checkbox"/>
George L. Graff	Briarcliff Man.	(914)502-2552		Edna Sussman	New York	(212) 213-2173	<input checked="" type="checkbox"/>
Richard F. Griffin	Buffalo	(716) 845-6000		Irene C. Warshauer	New York	(212) 695-1004	<input checked="" type="checkbox"/>
James E. Hacker	Latham	(518) 783-3843	<input checked="" type="checkbox"/>	Hon. Leonard Weiss	Albany	(518) 447-3200	<input checked="" type="checkbox"/>
A. Rene Hollyer	New York	(212) 706-0248	<input checked="" type="checkbox"/>	Peter H. Woodin	New York	(212) 607-2761	
David R. Homer	Albany	(518) 649-1999	<input checked="" type="checkbox"/>	Michael D. Young	New York	(212) 607-2789	



**Check preferred available dates or
schedule appointments online
directly with the state's top neutrals**

Visit www.NYMediators.org/quicksearch

This free web service funded by our New York members

The National Academy of Distinguished Neutrals is an invitation-only professional association of over 900 litigator-rated mediators & arbitrators throughout the US and Neutral Database Partner to the national trial bar (AAJ) & defense bar (DRI). For more info, please visit www.NADN.org/about

(paid advertisement)

Corporate Counsel Section Committee Chairpersons

CLE and Meetings

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

Steven G. Nachimson
Compass Group USA, Inc.
3 International Drive, 2nd Fl.
Rye Brook, NY 10573
steven.nachimson@compass-usa.com

Diversity

David S. Rothenberg
Goldman Sachs Family Office/
The Ayco Company L.P.
200 West Street, 40th Fl.
New York, NY 10282
david.rothenberg@gs.com

INSIDE/ Publications

Jessica D. Thaler
410 Benedict Ave.
Tarrytown, NY 10591
jthaleresq@gmail.com

Membership

Jana Springer Behe
NYSTEC
540 Broadway, 3rd Fl
Albany, NY 12207
behe@nystec.com

Joy D. Echer
Foot Locker, Inc.
Law Department
112 West 34th Street
New York, NY 10120
jecher@footlocker.com

Pro Bono

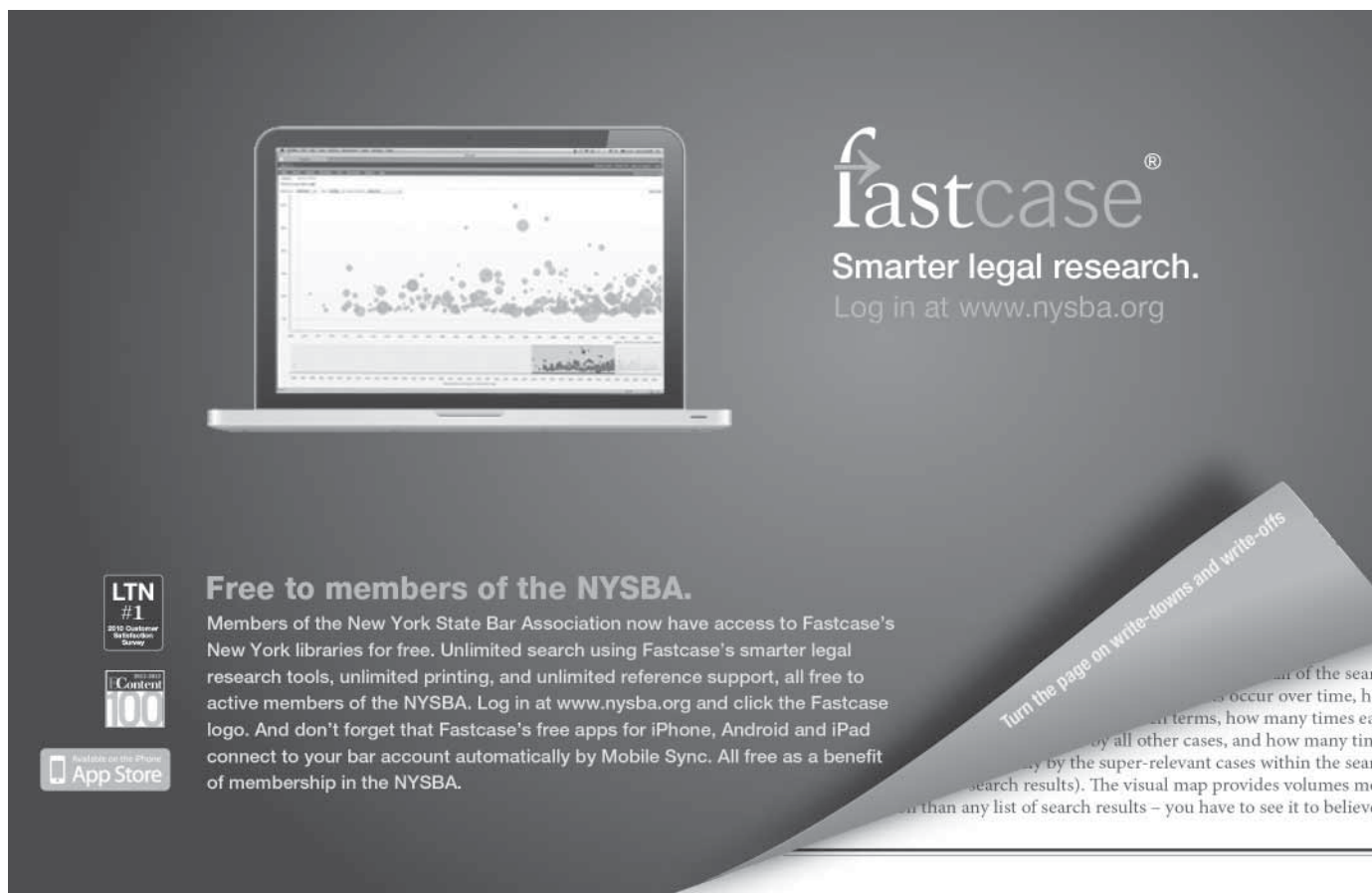
Cynthia Beagles
The American Kennel Club, Inc.
260 Madison Avenue
New York, NY 10016
ccb@akc.org

Steven R. Schoenfeld
DelBello Donnellan Weingarten Wise
& Wiederkehr, LLP
One North Lexington Avenue, 11th Fl.
White Plains, NY 10601
SRS@ddw-law.com

Technology and New Media

Fawn M. Horvath
Macy's, Inc.
11 Penn Plaza, 11th Fl.
New York, NY 10001
fawn.horvath@macys.com

Natalie Sulimani
Sulimani and Nahoum, P.C.
116 West 23rd Street, Ste. 500
New York, NY 10011
natalie@sulimanilawfirm.com



fastcase[®]
Smarter legal research.
Log in at www.nysba.org

Free to members of the NYSBA.

Members of the New York State Bar Association now have access to Fastcase's New York libraries for free. Unlimited search using Fastcase's smarter legal research tools, unlimited printing, and unlimited reference support, all free to active members of the NYSBA. Log in at www.nysba.org and click the Fastcase logo. And don't forget that Fastcase's free apps for iPhone, Android and iPad connect to your bar account automatically by Mobile Sync. All free as a benefit of membership in the NYSBA.

LTN #1
2013 Customer Satisfaction Survey

Content 100
2013-2014

Available on the iPhone
App Store

Turn the page on write-downs and write-ups



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

ADDRESS SERVICE REQUESTED

PRST STD
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.

Accommodations for Persons with Disabilities:

NYSBA welcomes participation by individuals with disabilities. NYSBA is committed to complying with all applicable laws that prohibit discrimination against individuals on the basis of disability in the full and equal enjoyment of its goods, services, programs, activities, facilities, privileges, advantages, or accommodations. To request auxiliary aids or services or if you have any questions regarding accessibility, please contact the Bar Center at (518) 463-3200.

© 2014 by the New York State Bar Association.
ISSN 0736-0150 (print) 1933-8597 (online)

Inside

Section Officers

Chairperson

Thomas A. Reed
1172 Park Avenue, Ste. 15-c
New York, NY 10128 • tareed1943@gmail.com

Chairperson-Elect

Natalie Sulimani
Sulimani & Nahoum P.C.
116 West 23rd Street, Suite 500
New York, NY 10011 • natalie@sulimanilawfirm.com

Vice-Chairperson

Cynthia Beagles
The American Kennel Club, Inc.
260 Madison Avenue
New York, NY 10016 • ccb@akc.org

Vice-Chairperson

Joy D. Echer
Foot Locker, Inc.
Law Department
112 West 34th Street
New York, NY 10120 • jecher@footlocker.com

Treasurer

Jeffrey P. Laner
77-10 34th Avenue
Jackson Heights, NY 11372 • jlaneresq@nyc.rr.com

Secretary

Yamicha Stephenson
Deloitte
1633 Broadway
New York, NY 10019 • yamicha.stephenson@gmail.com