INSIDE THIS PUBLICATION:

Fitting Social Media Into Your e-Discovery Regime
Autonomy: The Social Side of Information Governance
The SEC Remains Behind on Social Media
KPMG: Risk Management in an Evolving World
NLRB Provides Guidance on Social Media Practices
Symantec: Education and Training Are Key to Proper Use of Social Media
Monitoring Employees’ Use of Social Media
Company Descriptions

Compliance in the Age of Social Media

An eBook publication in conjunction with Autonomy, KPMG, and Symantec.
1,351 tweets about your company.  
Fortunately, you were part of the conversation.

Social media is a 24x7x365 conversation that offers tremendous marketing opportunities—but only if you can control the “voice of the company.” KPMG can help you manage the conversation through effective social media governance programs. So you can monitor the chatter across multiple channels, provide guidance to employees, and refine your messages. That’s a conversation worth having.

Contact Sanjaya Krishna at skrishna@kpmg.com or Phil Lageschulte at pjlageschulte@kpmg.com

kpmg.com
Inside this eBook:

Fitting Social Media Into Your e-Discovery Regime 4
Autonomy: The Social Side of Information Governance 6
The SEC Remains Behind on Social Media 8
KPMG: Risk Management in an Evolving World 10
Cura Software: Improve Risk Management Maturity 12
NLRB Provides Guidance on Social Media Practices 12
Symantec: Education and Training Are Key to Proper Use of Social Media 14
Monitoring Employees’ Use of Social Media 16
Company Descriptions 19
By Jaclyn Jaeger

Social media may be a lucrative new tool for businesses that should be embraced, but other elements of the business world are eternal constants—and lawsuits are one of them. And fitting that new world of social media into the existing order of litigation and e-discovery is not easy.

Unlike traditional data—Word documents, spreadsheets, e-mail messages—in which companies can usually pinpoint where information exists and how to retrieve it, data posted on social networking sites is not physically stored on the user’s computer, or even on the company’s servers. In fact, social networking data in “the cloud,” can exist anywhere, making social media e-discovery a practical impossibility.

“Businesses know how important it is to protect and preserve e-mail, IM, spreadsheets, and other unstructured information,” says Greg Muscarella, senior director of product management for Symantec’s Information Management Group. “Now they need to recognize that information flowing through social networks is equally important.”

According to the findings of a recent study, “Trends in e-Discovery: Cloud and Collection,” conducted by Clearwell and the Enterprise Strategy Group, 27 percent of respondents included social media applications as part of e-discovery in 2010, and 58 percent expect to in 2011. The three types of social media that respondents cited the most were Facebook (79 percent); Twitter (64 percent); and LinkedIn (55 percent).

The study further concluded that discovery in cloud-based applications—that is, computer programs and data that exist on the Internet, rather than the computers in your office—will parallel the expected rise in social media discovery. When asked to forecast the cloud-based application that would be included most in e-discovery, 61 percent of respondents cited collaboration suites like Microsoft SharePoint. They also cited cloud e-mail (54 percent) and e-mail archives (29 percent).

The expected rise in social media discovery, combined with tougher data preservation laws, underscores why companies need to gain a better understanding of their employees’ social media activities, rather than banning or prohibiting them. “You have to learn to coexist with it, and to do that you have to have an appropriate strategy,” says Sheila MacKay, senior director of e-discovery consulting for Xerox Litigation Services, the e-discovery division of Xerox Corp.

Philip Favro, a discovery attorney at IT security giant Symantec, agrees. Social media can be tremendously useful to companies if used properly, he says—and likewise, “they can be a tremendous headache if not properly addressed.”

Courts have generally ruled that data on social network-
the right way to approach social media, because there are so many different avenues and aspects to it that it’s important to have all parties at that table for a strategy session,” MacKay says.

When moving to the cloud, many e-discovery experts advise companies to store only relevant data. Oftentimes companies move their data to the cloud because it offers ample data storage at a cheap price, “but you don’t want to have to cull through unlimited amounts of data when you have to respond to an e-discovery litigation event,” Favro says.

It’s also critical to consider how secure that data is as it floats into and out of the cloud, and that the right encryption tools are in place to prevent hackers from getting in, Favro adds. He offers a list of questions to consider while deciding what cloud provider to choose:

» Does the cloud provider offer a de-duplication function that allows users to eliminate redundant data?
» Can it automatically delete unnecessary data in accordance with a data retention policy? Conversely, will the cloud provider agree to a legal hold policy so that data isn’t deleted before the retention policy is up?
» Can you retrieve data in a timely fashion in the event of a discovery request?
» What types of security measures does the cloud provider have in place? Passwords, firewalls? Anything else?
» Is the data being stored in a physically secure facility?
» Does the facility have a fire suppression system? Does it have backup in case of a power outage, fire, or some other disaster?

“Cheap storage isn’t enough. It needs to be intelligent, and it needs to be secure,” Favro says.

The best-case scenario would be if the cloud provider’s document retention policy aligns with the company’s document retention policy. Larger cloud providers—such as Amazon, Google, and Microsoft—may not provide that option, Carter says. Depending on the company’s needs, it may be better to enlist the help of a smaller cloud provider, she says.

The good news is that companies are starting to see guidance in this area, MacKay says. For example, the Sedona conference, a law and policy think tank, recently published a paper on best practices around managing information and records in the electronic age. As a starting point, MacKay says, “Organizations can take those ideas and use them to help implement different policies and procedures in-house.”

The following chart from Clearwell shows what applications are most commonly being delivered through SaaS or the cloud:

<table>
<thead>
<tr>
<th>Applications Organized Have Deployed or Expect to Deploy via the SaaS Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM (Customer Relationship Management)</td>
</tr>
<tr>
<td>E-mail</td>
</tr>
<tr>
<td>Collaboration/file sharing</td>
</tr>
<tr>
<td>Project management</td>
</tr>
<tr>
<td>Data protection (backup/recovery, data archive, etc.)</td>
</tr>
<tr>
<td>Sales force automation</td>
</tr>
<tr>
<td>Security (anti-spam, anti-virus, etc.)</td>
</tr>
<tr>
<td>Human resources</td>
</tr>
<tr>
<td>Internet/e-mail marketing</td>
</tr>
<tr>
<td>Accounting/financial</td>
</tr>
<tr>
<td>Business analytics</td>
</tr>
<tr>
<td>Industry-specific applications</td>
</tr>
<tr>
<td>Content management/document management</td>
</tr>
<tr>
<td>Legal (e-discovery, case management, etc.)</td>
</tr>
</tbody>
</table>

What specific applications has your organization currently deployed or does it expect to deploy via the SaaS model? (Percent of respondents, N=335, multiple responses accepted)

Source: Clearwell Study: Trends in e-Discovery.
The Social Side of Information Governance
4 Best Practices for Corporate Compliance & Risk Officers

In just a few years, social media has gone from a cutting edge phenomenon to a mainstream channel that corporations use to engage clients, partners, and vendors. As a result, Chief Compliance and Risk Officers must explore this pervasive communication channel and understand how its use may impact the organization’s ability to manage risk.

Changing Legal Requirements
As the nature of communication between employees, customers, and businesses evolves, corporations are leveraging social media networks and using mobile devices more frequently. Gartner predicts that by 2014, social networking services will replace email for interpersonal business communications for 20 percent of business users.1

Beyond email, IM, and chat, regulations now include audio (COBS 11.8) and social media channels (FINRA 10-06 and others now in development). Recent case law in the U.S. and Canada has highlighted the need to manage social media usage due to the potential discoverability of ESI under the FRCP, Canadian civil procedure rules, and other regulations.2 Moreover, social media data needs to be managed pursuant to compliance regulations, such as FINRA Regulatory Notice 10-06.

Interactions in the Spotlight
Enterprise content is growing exponentially and is increasingly “unstructured”, as in the case of social media, email, video, audio, text, and web pages. The prevalence of these unstructured data types in the enterprise are causing a shift from a “document” centric view of compliance, discovery, and information management, to models based on interactions. As a result, compliance officers must find new ways to increase information control and visibility. The following questions can help determine what to consider when creating a plan for social media governance:

» How is the organization, including employees, interacting on social networks?
» What communication channels are we using?
» What are we obligated to preserve?
» How do we enforce and monitor compliance policies?

Traditional methods like relational databases only operate on structured data, which constitutes just 15 percent of information. They ignore human “unstructured” information, which now represents 85 percent of data. Managing all data enterprise wide requires a system that understands all content regardless of format, and can apply consistent policies in real time. Effectively leveraging social media while protecting the organization from non-compliance requires a social media governance plan that allows compliance departments to:

✓ Extend existing compliance, supervision, and surveillance practices to interactive content
✓ Perform conceptual search and policy-based monitoring of all information—inside and outside the firewall
✓ Establish social media usage policies and procedures, and then train staff on the particulars
✓ Preserve and collect relevant social media content for compliance and litigation purposes

Traditional Methods Fall Short
Managing social media involves many different factors, including volume of data, content type, use of language, and the nature of the communication (such as conversational or slang-based). Traditional methods like manual review and monitoring are labor intensive and ineffective. In addition, volumes have been written on the limitations of keyword search and the benefits of conceptual search and contextual analysis to help provide an understanding of content and automate processes.3

A vital part of any comprehensive social media governance plan must also consider all content and access methods in play, as users connect via smartphones and tablets. While yesterday’s technology could not readily record interactions, now it not only can memorialize interactions in real time, but do so without awareness by participants. Understanding the meaning of these new interactions is the only effective way to govern content flowing across a range of interaction channels.

Social Media Governance Best Practices
Interactions with social media may not always occur on a corporate network or controlled device, and more importantly, content may be stored with a third party, such as Facebook or Twitter. This means current corporate policies may not extend to social media—a dynamic that

1 See http://www.gartner.com/it/page.jsp?id=1467313
Primary categories of interactions. Most regulated organizations are taking a measured approach to social media, starting with a limited number of employees and approved social media sites. Companies are focusing first on categories of interaction models or capture methods. Next, they can become familiar with how employees are interacting, and explore options to govern the full breadth.

- **Inside-Based Interactions:** These social media interactions occur within a corporate network, or on a corporate-controlled device, allowing interactions to be captured or controlled on the device and at the network layer. Companies can capture interactions without employee assent or approval, assuming policies exist regarding monitoring or collecting information stored or transmitted on corporate devices and networks.

- **Moderated Interactions:** These interactions occur on corporate-maintained social media accounts on sites such as Facebook or Twitter, and the organization itself is essentially the “owner” of the page and associated interactions.

- **Outside-Based Interactions:** These interactions occur off an organization-controlled device or network. For organizations maintaining a policy permitting employees to engage in business conduct, they have two options for governing and monitoring these interactions:
  - **Individuals can “Opt-In” or register a particular social media account, granting the governance application the authority and credentials to see and capture content.**
  - **Corporations can use solutions that monitor aggregated feeds of publically available information (Twitter feeds, LinkedIn and Facebook sites, blogs, forums, third-party websites, and news sites) to learn what is said about the corporation, its people, or products.**

Best Practice #4: Focus on solutions that can establish what something means, and understand how it relates to potential risk for an organization.

Capturing all interactions provides limited value as it only creates more content to govern. Where compliance officers can derive value is in mitigating risk and identifying insights in interactions to increase customer service or promote products. Given the volume of interactions, their brevity (think a 140-character Tweet) and complexity (audio and video), solutions must be able to find relevant patterns and relationships in the information to take action. Understanding the meaning of social media interactions is more important than simply capturing whatever someone can create.

Conclusion

Social media presents unique opportunities for all organizations, even the most tightly regulated or highly litigated. As it evolves, social media only becomes more pervasive, creating new methods for interacting with a variety of audiences. At the same time, social media interactions present unique risk, requiring organizations to develop governance models mindful of legal and regulatory guidelines. This new understanding also creates obligations, while prohibiting or limiting some types of conduct. More importantly, compliance officers must look beyond the ability to capture interactions, and instead focus on what it all means.

---

4 At this point there is limited guidance on whether third parties must assent to monitoring or capture of social media, either the site owner itself or third-parties posting to that site. This is an area of law that will likely remain unsettled for some time.
The SEC Remains Behind on Social Media

By Bruce Carton
Compliance Week Columnist

The Securities and Exchange Commission continues to dip its toe into the social media waters, but it’s doing so in such a cautious, disjointed way that it undermines the usefulness of powerful online communication tools.

The SEC’s stumbling over social media are surprising, given the aptitude it has shown for online communication for the last several years. In securities enforcement, for example, the SEC’s Website has been a tremendous source of information, and includes pages that list all of the agency’s litigation releases, press releases, and administrative proceedings. This information is extremely useful, and lawyers, reporters, investors, and countless others interested in the SEC and enforcement issues visit these Web pages daily. To the SEC’s credit, these Web pages are well maintained and reflect a clear commitment by the SEC to leveraging the Web to get the word out about its work in this area.

These days, however, a growing mass of people prefer to get their news streamed to them via social media sites such as Twitter or Facebook, rather than actively surfing the Web. With about 15 minutes of effort, the SEC could set up automatically generated, real-time feeds on Twitter or Facebook for each of the information sources discussed above (and many more), but to date these feeds do not exist.

Worse, the few feeds that the SEC has set up provide an unfocused mix of data and, in at least one case, have not been updated in months. Finally, and perhaps most perplexing of all, the baby-steps the SEC has taken in the area of social media are virtually invisible to the public because the SEC’s homepage has not a single visible reference or link about any of its social media offerings.

Here is what I’ve seen from the SEC in the area of social media to date, and how it can quickly and easily improve on these efforts for the benefit of investors:

1. Twitter

   **What the SEC has:** Right now the SEC has three Twitter feeds:

   » **SEC_News:** This feed includes a mish-mash of information from the SEC. It contains no litigation releases, no administrative proceeding releases, and a tiny subset of press releases—but of the seven SEC press releases issued in the second half of April 2011, only one is included on SEC_News. It also includes random information about things like meetings that are going on that many people probably don’t care much about (For example, consider this tweet: “WATCH LIVE: SEC Open Meeting REGARDING Product Definitions Contained In Title VII Of The Dodd-Frank Act).”

   » **SEC_Investor_Ed:** This feed includes a bevy of announcements about what the SEC’s Office of Investor Education is doing. (For example, the SEC tweeted: “Office of Investor Education and Advocacy’s investing guidance for parents.”) But it contains even fewer press releases, and no litigation releases or administrative proceedings.

   » **SEC_Jobs:** This feed provides information on jobs that are available at the SEC. More accurately, this feed used to provide information on jobs that are available at the SEC. Although it was once updated throughout the day with new positions, SEC_Jobs has not been updated in nearly two months as of early May. Either no new jobs are available at the SEC these days, or the SEC has lost interest in the SEC_Jobs feed.

   **What the SEC needs:** First and foremost, the SEC should have separate Twitter feeds for each of its main streams of information. This would allow users to receive exactly the type of information they want, and no more. In the enforcement world, this would mean, at a minimum, separate and dedicated Twitter feeds for litigation releases, press releases, and administrative proceedings. Beyond the area of SEC enforcement, I believe additional SEC Twitter feeds for proposed rules, final rules, and no-action letters would also be useful and would garner a heavy following. This should be a very simple task, as there are many free services that permit Websites to have newly added content automatically posted to a Twitter feed.

   Interestingly, in 2009 the SEC actually did introduce a very useful “SEC_Actions” feed on Twitter that was dedicated solely to announcing new Litigation Releases, as I sug-
The feed, however, went dead after about five weeks. When I asked the SEC in 2009 why it had stopped updating the SEC_Actions feed, an agency spokesperson told me that this was because the SEC was “focusing on our investor education, news, and jobs Twitter feeds for now.”

As I wrote at the time, this explanation made little sense to me, given that the SEC_Actions Twitter feed could easily be wired to update automatically when the SEC updated its Litigation Releases page:

I don’t want to get off on a rant here, but to me, that is kind of like saying you’re not using your left turn signal while driving because you are “focusing” on the right turn signal, the gas pedal and the brake. That is to say, with about .0000001 percent additional effort, you could keep posting the SEC enforcement actions to @SEC_Actions and “maintain focus” on the other feeds.

Eighteen months later, the SEC has yet to add a single new Twitter feed and seems to have stopped “focusing” on its dormant SEC_Jobs feed.

2. **Facebook**

What the SEC has: A search for “Securities and Exchange Commission” on Facebook brings up a single page, with a seal and a brief description of the SEC from Wikipedia. It doesn’t appear to be the official Facebook page of the SEC. It contains almost no other links or information and is followed by just 262 people. That is the only SEC-related page on Facebook I could find.

What the SEC needs: Facebook has more than 500 million active users. Do you think some of them might be interested in the SEC? I do!

The SEC should follow the example of the Department of Justice, which revamped its Website last year to, among other things, promote its new presence on Twitter, Facebook, YouTube, and even MySpace. The Justice Department’s Facebook account already has more than 21,000 fans, and is regularly updated with key announcements and initiatives. The SEC could easily do the same.

3. **YouTube**:

What the SEC has: The SEC conducts and participates in many meetings, conferences, speeches, and other events that are videotaped. It makes perfect sense that the SEC would have its own YouTube channel where all of these videos could be archived. In fact, I was quite surprised to learn while researching this column that the SEC already does have such a channel—you’ve just never heard of it. Even people like me who follow and write about the SEC on a daily basis have never heard of it. But I’m here to tell you it does exist—visit http://www.youtube.com/user/SECViews if you don’t believe me.

What the SEC needs: Some form of communication with the rest of the world that this YouTube channel exists!

The Justice Department provides a good model for the SEC to follow in the social media area. On the homepage of its recently revamped website (www.justice.gov), there is a prominent box that reads “Stay Connected” and displays the well-known icons for Twitter, Facebook, YouTube, and MySpace. Clicking on any of those icons takes the user to the DoJ’s pages on those social media sites. Making it easy for interested parties to find you on social media seems like an obvious thing to do, but it is a step that the SEC and many other entities now venturing into this new world sometimes neglect.

In short, my review shows that the SEC now has two marginally useful and unfocused Twitter feeds; one “Jobs” Twitter feed that has not been updated in two months; no dedicated Twitter feeds for its most useful streams of information; a YouTube channel that almost nobody in the world knows about; and no official Facebook account. It is time for the SEC to raise its game in the world of social media, and start using these tools to their full potential to better educate and engage investors and the public.

---

**RECENT COLUMNS BY BRUCE CARTON**

Below are recent columns by Compliance Week Columnist Bruce Carton. To read more from Carton, please go to www.compliance-week.com and select “Columnists” from the Compliance Week toolbar.

**SEC Struggles With Inadequate Funding, Old Technology**

SEC Chairman Mary Schapiro has gone to Congress to argue that the agency is starved of resources and without a budget increase will be unable to carry out some of the functions assigned to it by the Dodd-Frank Act. Inside, Columnist Bruce Carton examines that claim and looks at a recent report that just might buoy Schapiro’s case.

Published online 04/12/11

**Is the SEC Clamping Down on the Non-Denial Denial?**

New signs are emerging from the SEC that it might revisit its longstanding policy of settling cases without requiring defendants to admit guilt, a potentially huge risk to executives later subject to private litigation. This week, Columnist Bruce Carton reviews how defendants fell back under SEC ire and how wise such a policy change may (or may not) be.

Published online 03/08/11
Risk management in an evolving world

The case for social media governance

Social media governance for the workforce

Corporate workforces are continually active on social networking sites through both personal and corporate platforms. This activity poses considerable reputational and revenue risks to organizations, such as data leakage via posting of work-related matters or other misuse of company intellectual property; reduction in workforce effectiveness; ineffective use of company bandwidth; and introduction of viruses and malware.

Organizations need to develop internal social media governance guidelines and inform employees and third-party entities about expectations regarding the use of social networking applications. At the same time, organizations will want to avoid a “big brother” reputation when it comes to workforce privacy, which can undermine employee trust. Balancing these competing concerns is a daunting task.

Studies show that employees spend significant time accessing and using social media while at work, using company devices. Security technologies can help address potentially detrimental issues of bandwidth utilization and virus/malware introduction. An added dimension of risk arises from workforce use of social media because most of these communications occur outside the direct control of the company, such as via home PCs and cell phones.

Therefore, organizations must develop a clearly defined policy for employee use of social media—on both the company’s enterprise technology and employees’ personal devices. This policy should address:

- Proper use of company devices to access external social media sites
- Guidelines and restrictions regarding disclosure of company matters, including product development and business plans; use of registered phrases and other intellectual property; and workplace conduct

- Training requirements for social media technologies
- Rights and responsibilities of the company to monitor workforce postings on social media.

Governing the “voice of the company” in social media

Without guidance, social media participants can become unsupervised company spokespeople. Thus, managing reputational risk remains a key challenge. The goal should be to design an enterprise-wide governance program that supports innovative adoption of social media tools while addressing their risks.

The first step in developing a market-facing social media program is to assess where you are now in your social media maturity. Management should then address the following issues:

- How will social media be used and by whom (both within the company and in the external marketplace)?
- Who is our target audience, and what behaviors do we want to drive?
- Who are the key staff who will be accountable for social media activity and what training will they require?
- What are our procedures for message approval so that key constituents—such as legal/regulatory, HR, and marketing/communications—can provide timely input?
- What crisis response practices have we established? Do they reflect the aggressive timeline that social media requires?
Managing risks and opportunities of social media

Social media technologies are continuing to evolve quickly, promising shifts in behavior by customers and workforces, new regulatory implications, and new risks and opportunities. Hence, organizations can use social media monitoring to inform their ERM programs.

Management must demonstrate a strategic understanding of how social media is evolving, how it affects the business, and what risks are associated with it. Questions to consider include:

» How can we listen and respond to what the marketplace is saying about the company?

» Have we identified and communicated the risks posed by our industry and market's use of social media related to information protection, reputation risk, and legal/regulatory risk?

» How effective are our controls around these risks?

Still, an organization's social media focus should not entirely be about mitigating risk. It must also examine trends to identify opportunities, such as establishing new electronic product channels for a specific target audience or creating a viral advertising campaign through social media vehicles. As a result, organizations need to monitor the major social media networks to identify both potential problems and major opportunities. This may require dedicated resources. It may also be a good idea to have a proactive plan for deciding when and how to respond to potential reputational issues being discussed in social media.

Conclusion

For most organizations, social media is at the beginning of its maturity curve. The rapid adoption of social media vehicles, combined with the rapid evolution of the Web 2.0 technologies, presents a complex challenge, especially for organizations in highly regulated industries.

Harnessing the power of social media can present specific risks to the organization. At the same time, the speed at which Web 2.0 technologies and market demands are evolving presents organizations with both great opportunity and greater need for governance.

Organizations need to build on their social media strengths while helping to ensure they have a strong foundation of governance—a foundation that enables them to:

» Identify social media risks and opportunities

» Enhance demonstrable controls of social media programs, satisfying both audit and compliance program demands

» Anticipate emerging regulatory compliance issues that may dictate their social media activities on a global basis

» Improve key third-party relationships with regard to social media technologies and utilization

» Gain stronger consensus among internal organizational areas affected by social media regarding strategic direction and risk management.

About the Authors

Sanjaya Krishna is a principal in KPMG’s Advisory practice and U.S. Digital Services Leader within KPMG’s Information, Communications and Entertainment practice. Sanjaya focuses on client challenges and opportunities related to emerging digital media areas, including social media.

Phillip J. Logeschulte is an IT Advisory partner and the Global and Americas Service Line Leader for KPMG’s IT Audit Services practice, with over 23 years experience providing information technology consulting and assurance services to clients across a variety of industries. He recently led an Information Systems Audit and Control Association (www.isaca.org) task force to publish a book on cloud computing, IT Control Objectives for Cloud Computing (2011 ISACA).

H. John Hair, an Advisory director in KPMG LLP’s IT Internal Audit practice, leads KPMG in the area of social media governance, with over 20 years of global development and operational management experience in new technology adoption. John has led KPMG teams providing audit/assessment reviews of social media programs for some of the firm’s key national clients.
NLRB Provides Guidance on Social Media Practices

By Jaclyn Jaeger

A new report from the National Labor Relations Board should be a big help for companies trying to craft practical (and legal) social media policies.

The report provides more detail on why some employees’ social media communications constitute legally protected activity, while others do not. It uses real-life cases, and serves as a warning to companies to exercise caution before taking any disciplinary actions against employees for what they say on sites such as Facebook, Twitter, and LinkedIn.

Issued in September by NLRB Acting General Counsel Lafe Solomon, the document cites 14 different cases, which collectively illuminate how the NLRB defines “protected concerted activity” under Section 7 of the National Labor Relations Act (NLRA) as it applies to employees’ use of social media.

Section 7 of the NLRA gives employees the right “to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all such activities.” The report further defines protected activity under the NLRA as two or more employees acting together to address a collective employee concern about terms and conditions of employment.

“It is my hope that this openness will encourage compliance with the Act and cooperation with agency personnel,” said Solomon in an accompanying statement.

Several companies have run afoul of the NLRA by disciplining employees for comments they made on social media sites. Non-union companies are especially vulnerable, because they aren’t used to dealing with labor organization issues. In fact, according to a report by the U.S. Chamber of Commerce, of the 129 cases involving some form of social media before the NLRB, a “significant percentage” involved non-union companies. “They may have never thought about the Act and how it might apply to them,” says Michael Eastman, executive director of labor law policy for the U.S. Chamber of Commerce.

The report examined one case—the first social media case to be decided by an administrative law judge—where the NLRB found that Hispanics United of Buffalo, a non-profit social services provider, wrongfully discharged five employees who had posted comments on Facebook criticizing their coworkers’ job performance and complaining about workload issues.

Four of the employees had made the comments in response to questions a coworker raised prior to meeting with a supervisor. In the report, the NLRB said this was a “textbook example of concerted activity,” since the discussion was initiated by one employee who was appealing to coworkers for assistance.

The NLRB further explained that it does not consider individual comments that don’t arise out of, or call for, concerted activity to be protected, even if they are employment related. “Employers certainly welcomed seeing that not every comment on Facebook is protected under the National Labor Relations Act,” says Eastman.

For example, a restaurant employee was discharged after complaining on his Facebook page about his employer’s tipping policy. Even though the posts related to terms and conditions of employment, it did not grow out of prior conversations with coworkers and there was no other evidence of concerted activity. In this case, the NLRB found in favor of the employer.

“Pure griping by one employee generally is not protected,” says Eric Meyer, a partner in the labor and employment practice at law firm Dilworth Paxson and author of The Employer Handbook Blog.

The NLRB report also indicated that the tone and language of a post—no matter how vulgar—does not influence whether it is protected or not. In one case, the NLRB found that an ambulance service unlawfully terminated an employee who posted negative remarks about her supervisor on her personal Facebook page. That she referred to her supervisor as a “scumbag” didn’t justify the employer’s actions.

“Regarding the nature of the outburst, the name-calling was not accompanied by verbal or physical threats, and the [NLRB] has found more egregious name-calling protected,” the report said. The NLRB pointed out that the supervisor’s unlawful refusal to provide the employee with a union representative and his unlawful threat of discipline provoked the employee’s Facebook postings.

The board is “clearly taking an aggressive position” on what qualifies as protected activity under the National Labor Relations Act, Meyer says.

Brian Hall, a partner of Porter Wright, agrees. “Because social media has become so prevalent, the board has identified this as a logical vehicle for pushing forward with its broad interpretation of protected rights,” he says. Rather than look at how the NLRB has decided each case individually, employers would be wise to look at the report as a whole, because it “gives a good flavor for what the board would decide not only in those particular cases, but on any number of other cases that might arise in the future,” he says.
Social Media Policies

In addition to cases challenging employers’ disciplinary actions against employees’ social media activities, the NLRB report also assessed cases where the board challenged employers’ social media policies as overly broad. According to the report, a social media policy cannot restrict wage discussions, corrective actions and discharge of coworkers, employment investigations, and disparagement of the company or its management.

A settlement reached in February where American Medical Response of Connecticut agreed to revise its policies provides two general examples of policy statements the NLRB will find unlawful. In the complaint, the NLRB found AMR’s blogging and Internet posting policy to be overly broad because it “prohibited employees from making disparaging remarks when discussing the company or supervisors, and from depicting the company in any media, including but not limited to the Internet, without company permission,” the NLRB stated.

Specifically, the NLRB took issue with the policy because it prohibited employees from posting photos in any form of media depicting the company in any way, including a company uniform or corporate logo. The NLRB concluded that this language “would prohibit an employee from engaging in protected activity.”

The board further concluded that the portion of the policy prohibiting employees from making disparaging comments when discussing the company or the employee’s superiors, coworkers, or competitors was unlawful, because it contained no limiting language to inform employees that it did not apply to Section 7 activity.

AMR declined to offer further comment regarding the settlement or its policies.

An acceptable social media policy does allow for limiting employees’ social media activity for the purpose of ensuring a consistent, controlled company message. For example, a policy that precluded employees from pressuring coworkers to connect or communicate with them via social media was valid as it was “narrowly drawn to restrict harassing conduct and could not reasonably be construed to interfere with protected activity,” the NLRB stated.

Employment lawyers say a safe approach is to include a disclaimer in the social media policy stating that the it will not be interpreted or enforced in a manner that would interfere with employees’ rights under the NLRA.

Indeed, employers will soon be making even broader disclaimers. The NLRB issued a rule, which goes into effect on Nov. 14, that says all private-sector companies whose workplaces fall under the NLRA will be required to post a notice alerting employees of their rights under the Act. Furthermore, companies that customarily post notices to employees regarding personnel rules or policies on an Internet or intranet site will be required to post the NLRB’s notice on those sites.

Employers will not be required to distribute the notice via e-mail, voice mail, text messaging, or related electronic communications, even if they customarily communicate with their employees in that manner.

While the NLRB report will go along way toward providing clarity on acceptable social media policy, the board’s positions have yet to be tested in court. An employer would have to challenge the NLRB for it to reach the federal appellate court level. The real question is “whether employers are really anxious to be the guinea pig for that case,” says Hall. “My guess is that it will be awhile before a case works its way through the system to get to the federal courts.”

In its report, the National Labor Relations Board spells out several examples that would make a social media policy overly broad. Specifically, companies are not allowed to prohibit:

» Any inappropriate or sensitive discussions about the company, management, or coworkers;
» Any social media post that constitutes embarrassment, harassment or defamation of the company or any employee, officer, board member, representative, or staff member;
» Any social media post that lacks truthfulness or might damage the reputation or goodwill of the employer, its staff or employees;
» Employees’ use of social media to communicate about company business, from posting anything that they would not want their manager or supervisor to see, or that would put their job in jeopardy;
» Revealing personal information, including through photos, regarding coworkers, company clients, partners, or customers without their consent;
» Employees from posting pictures of themselves in any media depicting the company in any way, including company uniform or corporate logo;
» Use of the company name, address, or other information on their social media personal profiles;
» Use of the employer’s logos and photographs of the employer’s store, brand, or product, without written authorization;
» Employees from using any social media that may violate, compromise, or disregard the rights and reasonable expectations of privacy or confidentiality of any person or entity; and
» Offensive conduct and rude or discourteous behavior, in the application to social media.

Source: National Labor Relations Board.
As the rise of social media changed the way your organization handles regulatory compliance and e-Discovery requests? If it hasn’t, it will.

Organizations large and small are learning the value of using social media to communicate with customers, partners, and employees. Social sites such as Facebook, Twitter, and LinkedIn are being tapped for everything from marketing programs to corporate communications to customer relationship management.

All this social media activity has IT departments worried—and with good reason.

According to a recent Symantec Social Media Protection Flash Poll, the typical enterprise experienced nine social media “incidents” in the past year, with 94 percent of the respondents saying they suffered negative consequences as a result. More disturbing, these incidents cost the typical company upwards of $4 million in the period.

That’s why it’s more important than ever to have a strong social media strategy and controls in place to prevent the release of confidential information, comply with regulations, and respond promptly to e-Discovery requests.

Understand the risks
What were the top social media incidents experienced by the typical enterprise last year? According to the Symantec poll, they were:

» Employees sharing too much information in public forums (46%)
» Loss or exposure of confidential or proprietary information (41%)
» Embarrassment or damage to brand or reputation (40%)
» Increased exposure to litigation (37%)
» Violation of regulatory rules (36%)

Respondents who experienced a social media incident also suffered the following negative consequences: reduced stock price, litigation costs, direct financial costs, loss of customer trust, and lost revenue.

Understand the changing e-Discovery landscape
Just how pervasive has social media become within the enterprise? Consider: Gartner Inc. has predicted that, “by year-end 2013, 50 percent of all companies will have been asked to produce material from social media Websites for e-Discovery.”

That’s in line with the results of another recent Symantec survey, which found that e-mail is no longer the primary source of information for an e-Discovery request. The 2011 Information Retention and eDiscovery Survey, which examined how 2,000 enterprises worldwide are managing ever-growing volumes of electronically stored information, determined that both structured and unstructured information sources outranked e-mail. As evidence of just how the eDiscovery landscape is evolving, nearly half of the respondents cited social media as being among their most frequently requested records.

The survey also found that companies employing best practices, such as automating the placement of legal holds and leveraging an archiving tool rather than relying on backups, fared dramatically better when it came to responding to an e-Discovery request. In addition, these top-tier companies were significantly less likely to suffer negative consequences than companies that lack a formal information retention policy. Specifically, top-tier companies were much less subject to court sanctions, compromised legal positions, and fines.

1 “Social Media Governance: An Ounce of Prevention,” Gartner; December 17, 2010
Key recommendations for addressing the challenges of social media

While there are many steps that can be implemented to address the challenges associated with social media, the following five are indispensable:

1. As with all corporate communications, develop a global plan for how you will engage in social media. This initial step is particularly important for organizations that are just now exploring the use of social media.

2. Educate and train employees regarding the social media plan. This should include instruction regarding what content may be posted to social networking sites and the internal process for doing so. Policies that describe the consequences for deviating from the social media plan should also be clearly delineated.

3. Identify and understand the legal or regulatory requirements specific to your industry; implement policies to address regulations that call for retention of social media content.

4. Consider deploying an archiving solution that enables the automatic capture and retention of social media content, especially if your industry is heavily regulated.

5. Implement a data loss prevention solution to provide another layer of protection to prevent confidential and proprietary information from leaving the company.

Symantec social media partners

Symantec works closely with several partners to capture social media communications and make it discoverable within the Symantec Enterprise Vault archiving platform and the Clearwell e-Discovery Platform. These partnerships provide customers with flexibility in the type of solution they choose (i.e., cloud-based vs. on-premise) and in the features that are offered. Depending on your needs, these partners—Actiance, CommonDesk, Globalnet, Hanzo, and Socialware—are able to capture and/or control social content across Facebook, LinkedIn, Twitter, Google+, Websites, YouTube, and many other social media vehicles.

For example, policies can be created to capture any communications from a corporate marketing Twitter account—sent and received. If more granular control is wanted, policies can be enforced that scan and check messages before being posted live to ensure end-user and regulatory compliance.

Conclusion

Recent surveys confirm that social media use is on the rise for almost all organizations. But as these companies increasingly share business-related information on social networks to communicate with customers, partners, and employees, the risk of publishing confidential information also increases. By following the steps outlined in this article, organizations can continue to access and share information through social networks while capturing and preserving it for legal and compliance purposes.

To learn more, download the Symantec Webcast, “The Impact of Social Media on IT and Legal.”

Want to follow the latest e-Discovery issues and trends? Read the Symantec e-Discovery 2.0 blog.
Monitoring Employees’ Use of Social Media

By Karen Kroll

Facebook currently boasts 700 million users, Twitter 200 million, and LinkedIn 100 million. Chances are your employees frequent at least one of these social media sites from time to time. And chances are compliance departments aren’t quite clear on what their oversight role can be when employees post something that mentions their employer.

Fear that employees will say things that could come back to haunt their employers certainly isn’t new, says Jack Greiner, a partner at law firm Graydon Head & Ritchey in Cincinnati; social media’s blistering speed and global scope simply have made employer’s concerns much more urgent. “The ability to control it has lessened a bit,” Greiner says.

So far the regulatory leadership on social media has emerged (as it often does) from the financial sector. The Financial Industry Regulatory Authority closely regulates how its member firms communicate to customers, and social media is no exception. FINRA Notice 10-06, “Guidance on Blogs and Social Networking Sites,” identifies two types of content on social media sites: static and interactive content.

Static content is relatively straightforward: An employee posts it somewhere online, and it remains there unchanged and available for all visitors to a Website to see. “As with other Web-based communications such as banner advertisements, a registered principal of the firm must approve all static content on a page of a social networking site established by the firm or a registered representative before it is posted,” the FINRA guidance says.

Interactive content, such as posts on LinkedIn or Twitter, doesn’t require prior approval—but FINRA does still require firms to supervise these communications, “in a manner reasonably designed to ensure that they do not violate the content requirements of FINRA’s communication rules.” FINRA offers several examples of what it considers appropriate supervision, such as reviewing a sample of employees’ posts, either before or after they appear online.

Those rules give financial firms several challenges. One is simply ensuring that they have a system in place to comply with FINRA’s monitoring requirements efficiently; in a world of smart phones and other mobile devices, manual review of employees’ online activity is nearly impossible.

Enter the software vendors, such as the Belmont, Calif.-based Actiance Inc. Its new product Socialite allows firms to monitor content posted by employees and to establish an approval process for potential changes to static content, says Sarah Carter, director of marketing. The reviewer can approve, reject, or suggest changes to the information that’s about to be posted, she says. Actiance also can archive the content. Socialite was designed to meet the guidelines of FINRA, as well as those issued by its northern counterpart, the Investment Industry Regulatory Organization of Canada, Carter adds.

The software works with more than 1,000 social media platforms and includes features specific to each. For example, when a FINRA-registered representative hits the “like” button in response to a Facebook post, regulators might view that as providing an endorsement, Carter says. Socialite can be configured to restrict employees’ ability to use that function.

Actiance has a partnership with LinkedIn that gives Actiance access to LinkedIn’s programming interface—the technical bridge that allows Socialite to monitor employees’ LinkedIn activity, including any updates employees make via devices not issued by the company, such as their personal mobile phones or laptops, Carter says.

A nifty idea for compliance departments, to be sure. But that monitoring ability still presents employers—particularly in regulated industries—with several potentially conflicting expectations about employees’ use of social media.

On one hand, “I own what I do as a private citizen,” says Eric Goldman, a law professor at Santa Clara University who studies technology issues. On the other hand, employees can use the sites to conduct communications that are regulated by FINRA and other authorities.

Several lawsuits have determined that employees are free to state their thoughts, and even to criticize their bosses or workplaces, using social and other media. “Employees can talk to each other about their work conditions, and if employers try to stop them, it can be a problem,” Greiner says.

A 2009 lawsuit in New Jersey involved two employees who were fired by the restaurant chain Houston’s after a manager was provided with the password to a private MySpace group employees had established to vent about their work conditions. The employees didn’t access the group at work. The jury found that the company had violated the Stored Communications Act and the New Jersey Wire Tapping and Electronic Surveillance Act, although they rejected the plaintiffs’ claim for invasion of privacy, according to the summary by the Citizen Media Law Project.

More recently, the National Labor Relations Board has begun investigating employees’ claims of termination over comments posted on social media sites, says Susan Freiwald, professor of law at the University of San Francisco.

At the same time, individuals working in regulated industries have been penalized for comments on social media sites that were deemed inappropriate. One case involved Jenny Quyen Ta, who was fined $10,000 and suspended from association with any FINRA member for one year. Among other things, “FINRA determined that Ta’s tweets were unbal-
DISCOVERY ACHIEVED
Symantec Enterprise Vault. Store, manage, and recover critical information.

Confidence in a connected world. Symantec.
anced, overwhelmingly positive, and frequently predicted an imminent price rise, and Ta did not disclose that she and her family members held a substantial position in the stock,” according to a FINRA statement.

Communications on employee-owned systems can be held to a higher standard of monitoring. According to the Electronic Communications Privacy Act, where a company owns a communication system such as a corporate network, it can monitor whatever flows through that network, Greiner says. What’s more, while experts generally recommend that companies let employees know that their communications are being monitored, they aren’t required to do so.

Laws are also changing to consider the blurring of lines between work and non-work activities. While it used to be that an employee’s location—whether at work or at home—at the time he or she sent a message was important in determining what regulations might apply to the communication, that’s no longer automatically the case, Greiner says. “When someone sends an e-mail, where they are when they send it isn’t all that relevant.”

What is relevant is the content of the message. For instance, the Securities and Exchange Commission prohibits employees from selectively disclosing material information about a company before announcing it publicly. If an employee violates that rule (Regulation Fair Disclosure) via social media, his employer probably has some liability, Greiner adds. In addition, “the FINRA regulations would limit the employee’s reasonable expectation of privacy,” Greiner says.

The most effective way to balance the various responsibilities is to ask for employees’ consent to be monitored, Greiner says. In addition, once a company establishes a monitoring policy, it must consistently follow through. If companies use monitoring only sporadically, or only to discipline certain groups of employees, that can create problems.

Making matters worse for compliance officers, there are still plenty of unsettled legal issues surrounding employee use of social media. The current regulations leave “a lot of gray areas,” Goldman says. Many electronic publication sites allow individuals to discuss their work and private lives simultaneously, without a good way to separate the two. “The whole regulatory structure needs to be rethought,” he adds.

Until then, employers need to be sensitive not only to the laws, but expectations, Freiwald says. “There’s the law and then there are norms. Companies run the risk of being seen as insensitive to employees’ privacy” if their monitoring is seen as overly aggressive. Given the speed with which news can travel—often via social networks—that’s a real risk.

---

**SUPERVISION OF SOCIAL MEDIA SITES**

The following excerpt from FINRA guidance answers the question: How must firms supervise interactive electronic communications by the firm or its registered representatives using blogs or social networking sites?

The content provisions of FINRA’s communications rules apply to interactive electronic communications that the firm or its personnel send through a social media site. While prior principal approval is not required under Rule 2210 for interactive electronic forums, firms must supervise these interactive electronic communications under NASD Rule 3010 in a manner reasonably designed to ensure that they do not violate the content requirements of FINRA’s communications rules.

Firms may adopt supervisory procedures similar to those outlined for electronic correspondence in Regulatory Notice 07-59 (FINRA Guidance Regarding Review and Supervision of Electronic Communications). As set forth in that Notice, firms may employ risk-based principles to determine the extent to which the review of incoming, outgoing and internal electronic communications is necessary for the proper supervision of their business.

For example, firms may adopt procedures that require principal review of some or all interactive electronic communications prior to use or may adopt various methods of post-use review, including sampling and lexicon-based search methodologies as discussed in Regulatory Notice 07-59. We are aware that technology providers are developing or may have developed systems that are intended to address both the books and records rules and supervisory procedures for social media sites that are similar or equivalent to those currently in use for emails and other electronic communications. FINRA does not endorse any particular technology. Whatever procedures firms adopt, however, must be reasonably designed to ensure that interactive electronic communications do not violate FINRA or SEC rules.

Firms are also reminded that they must have policies and procedures, as described in Regulatory Notice 07-59, for the review by a supervisor of employees’ incoming, outgoing and internal electronic communications that are of a specific subject matter that require review under FINRA rules and federal securities laws, including:

- NASD Rule 2711(b)(3)(A) and NYSE Rule 472(b)(3), which require that a firm’s legal and compliance department be copied on communications between non-research and research departments concerning the content of a research report;
- NASD Rule 3070(c) and NYSE Rule 351(d), which require the identification and reporting of customer complaints; NYSE Rule 401A requires that the receipt of each complaint be acknowledged by the firm to the customer within 15 business days; and
- NASD Rule 3110(j) and NYSE Rule 410, which require the identification and prior written approval of every order error and other account designation change.

Source: FINRA Guidance on Social Networking Sites.
Autonomy Corporation, an HP Company, is a global leader in software that processes human information, or unstructured data, including social media, email, video, audio, text and web pages, etc. Autonomy’s technology manages and extracts meaning in real time from all forms of information, both unstructured and structured, enabling companies to leverage their data assets. Autonomy’s product portfolio helps power companies through enterprise search analytics, business process management and OEM operations. Autonomy also offers information governance solutions in areas such as eDiscovery, content management and compliance, as well as marketing solutions that help companies grow revenue, such as web content management, online marketing optimization and rich media management.

Autonomy’s solutions are used by more than 25,000 customers including 87 of the Fortune 100, 10 of the top 10 financial services firms, 75% of the global 100 law firms, 9 of the top 10 pharmaceutical companies and many government agencies. Over 400 of the world’s leading technology companies embed Autonomy’s technology in their products. Autonomy also owns the largest private cloud of diverse data, with 31 Petabytes of information.

Please visit www.autonomy.com to find out more.

KPMG LLP, the U.S. audit, tax and advisory services firm, operates from 87 offices with more than 23,000 employees and partners throughout the U.S. Our purpose is to turn knowledge into value for the benefit of our clients, our people, and the capital markets. KPMG LLP is a member firm of KPMG International, a Swiss cooperative. The member firms of the KPMG International network have 137,000 professionals operating in 144 countries.

Symantec is a global leader in providing security, storage and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information, technology infrastructures and related processes against more risks at more points, more completely and efficiently than any other company. As the world’s fourth largest independent software company and backed by the Global Intelligence Network, our unique focus is to eliminate information, technology and process risks independent of device, platform, interaction or location. Our software and services protect completely, in ways that can be managed easily and with controls that can be enforced automatically – enabling confidence wherever information is used or stored.

**COMPLIANCE WEEK**

Compliance Week, published by Haymarket Media, Inc., is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has quickly become one of the most important go-to resources for public companies; Compliance Week now reaches more than 26,000 financial, legal, audit, risk, and compliance executives.
Autonomy Social Media Governance
A Trusted Link in the Compliance Chain

Autonomy is the undisputed compliance leader, providing a single platform that seamlessly analyzes and manages more electronic interactions than all other providers combined. Autonomy's unique Meaning Based technology recognizes concepts, patterns and relationships within all types of human information. With Autonomy, businesses can leverage the value of social networks with the complete control and visibility required to manage the inherent risk in today's interactive world.

Leverage the Strength of the Autonomy Chain:
- Securely manages 31 petabytes of content
- Ingests over 1.2 billion objects each month
- Analyzes and enforces policy against 400 million interactions each month
- Trusted vendor by 10 of the top 10 financial services firms
- De facto standard for global enterprises, securities firms, and regulators

Protect your organization with Autonomy Social Media Governance.
Find out more at www.autonomy/protect