

ARMA International's

hottopic

THE BIG PICTURE

Creating a Strategy for Organizational Use of Social Media



www.arma.org



twitter

Information Governance



RSDig (RSD InfoGov)

Are u ready to ready to respond to [#eDiscovery](#)?



RIM Manager (Records Manager)

Help! [@RSDig](#) I need help to prepare for litigation.



RSDig (RSD InfoGov)

Are u SURE u aren't over-retaining information?



ComplianceMgr (Compliance/Risk Manager)

I have to reduce business risk



RSDig (RSD InfoGov)

Start by making your [#compliance](#) team happy with defensible disposition :-)



IT Manager (VP of IT Infrastructure)

Hey, I have way too many [#ECM](#) systems to manage



RSDig (RSD InfoGov)

Use **RSD GLASS 2** ensure policy is enforced **across** information silos and regulatory jurisdictions



RIM Manager (Records Manager)

Thanks. **+1 RT** [@RSDig](#): Use **RSD GLASS 2** ensure policy is enforced **across** information silos and regulatory jurisdictions

Trending topics:

[#InformationGovernance](#)
[#CentralizedPolicy](#)
[#PolicyEnforcement](#)
[#eDiscoveryReadiness](#)
[#RepositoryAgnostic](#)
[#MultipleJurisdiction](#)
[#LifecycleManagement](#)

Follow RSD InfoGov on Twitter [@RSDig](#)

Don't miss updates from RSD InfoGov. Sign up today and follow your interests!



For more information, please visit www.rsd.com or scan the QR code.

THE OFFICIAL SPONSOR



of Information Governance



Collaborate

to Develop an Effective Social Media Policy

Paula Harris, CRM

Information assets have become the new currency for successful enterprises and, in some cases, outweigh the value of physical assets. This places records and information management (RIM) professionals in the midst of a unique time and opportunity to add value to their organizations.

At the same time, emerging technologies impacting the management of these information assets are evolving rapidly and, in some cases, fundamentally changing the way RIM professionals work. The introduction of social media within the business environment, for example, represents a sea change that is comparable to the introduction of personal computers, the

Internet, and e-mail.

This provides RIM professionals a prime opportunity to effectively partner with IT, legal, and other business units to manage the content being delivered through social media channels.

Social Media: The Business Imperative

Business drivers for leveraging social media vary by organization, but the most common ones are:

- **Customer engagement** – Social media's reach and level of engagement with consumers and customers are unprecedented. Whether using Facebook to engage a brand community, leveraging Twitter to

inform constituents of coupons or other cost-saving opportunities, or utilizing LinkedIn to connect employees, the old ways of working are drifting away.

Print media is quickly being replaced by online content. Social media presents a unique opportunity to consumers to have a more personal and immediate experience with the brands and services they use. As a result, social media provides a channel to create more brand loyalty and ultimately, to enhance revenue generation.

- **Recruiting and retaining employees** – The demographics of the workplace are changing, and astute leaders realize the workforce of

today and tomorrow expect to use at work the same productivity tools they use at home.

• **Revenue enhancement and market presences** – Social media is relatively easy and inexpensive to deploy. An organization's competitors can leverage social media to reach millions of people almost instantly to encourage them to buy their products instead. Organizations that do not participate could lose their competitive advantage, which ultimately affects their bottom line.

The success of an organization's social media strategy and policy is

its risks. RIM professionals that have done their homework in this area will not only be able to support the organization's business objectives, they will also raise their visibility as "go to" people that can be relied upon to provide assistance on future initiatives.

Social Media: Policy Development Considerations

Once the benefits for using social media have been identified and vetted by the business, RIM professionals, in collaboration with IT and legal, can assess the risks and determine strategies to minimize them.

following, though, is a sampling of the regulatory agencies that establish rules and regulations that could affect an organization's social media strategy and policy:

- The Federal Trade Commission and the conduct of spokespersons
- The Financial Industry Regulatory Authority and electronic communications
- The Security and Exchange Commission related to broker-dealer organizations
- The National Labor Relations Board and communications permissible about the workplace
- Data privacy considerations by federal, state, and international governing bodies to protect the personally identifiable information of such entities as employees, customers, suppliers, and business partners
- Intellectual property protections for company-specific proprietary information (e.g., trademarks, research, and development) and obligations to protect the rights of others (e.g., copyrights)
- The Digital Millennium Copyright Act related to copyright protection
- Title VII protections against discrimination
- First Amendment freedom of speech
- The Fair Credit Reporting Act
- Equal Employment Opportunity
- Commission protections against discrimination

Remember, many regulations were promulgated prior to the use of social media, and the judiciary is playing catch-up on their application to social media. Therefore, as with RIM generally, it is imperative to stay abreast of regulatory and judicial trends to help ensure the organization's policy is current.

Records Management Issues

Applying information lifecycle management to content on social media can pose significant challenges. So, an organization should answer the following:

The success of an organization's social media strategy and policy is predicated upon a well-thought-out business case.

predicated upon a well-thought-out business case. While the organization's leadership team is responsible for articulating the organization's vision for using social media, it will depend upon those individuals with information governance expertise to partner with them to ensure that vision is realized with as little risk to the organization as possible.

However, the RIM staff may not be thought of as that business strategy partner; it may be perceived as having expertise only in the areas of retention and storage. To change this perception, the RIM team must be well-versed in all things social media, which includes understanding trends in how individuals are using social media and the rules that govern its usage.

The RIM team must also temporarily remove its compliance hat and engage the leadership team so it will understand the goals for using social media and can communicate

As with retention schedule development and implementation, there is no one-size-fits-all solution, and, as with any policy, developing social media policy should not be done in a vacuum. RIM professionals can leverage their relationships with other departments to create a policy team to address the myriad issues surrounding social media.

Working with leadership, as well as with human resources, the policy team should consider the organization's culture (the ways work is being accomplished) in relation to its regulatory environment and its risk tolerance level to determine how to structure and implement the policy.

Regulatory Environment

Numerous regulations govern social media sites, and a complete list goes beyond the scope of this article. Suffice it to say, each organization must make a determination as to what regulations govern its activities. The

- Is the information being placed on the social media site the official business record, or is it a copy with the official record being retained in another location?
- Who will own the information being posted?
- What retention classification will be assigned?
- How will content be managed over its life cycle?
- How will postings subject to legal hold be preserved?
- Who will be responsible for monitoring the site for changes in content?
- What are the terms and conditions of the social media sites being used?
- Do these sites retain information indefinitely?
- How will the sites respond for requests for information resulting from investigations or during litigation?
- How will the sites respond to misuse or the posting of inappropriate content?

Policy Implementation Strategies

Again, a one-size-fits-all social media policy does not exist. A software company may have very different rules of engagement for its employees and the management of its site than a financial institution does. However, by attending conferences, reviewing social media policies that are publicly available, and seeking out the policies of similar organizations, RIM professionals will expand their knowledge and be better equipped to help identify any risks or issues the organization may otherwise fail to consider.

Finally, before “reinventing the wheel” with its social media policy, RIM professionals should review the organization’s current compliance and governance standards that may support and/or cover the same or similar risks presented by social

media. For example, an organization may have a code of conduct that covers acceptable electronic usage policies.

Several categories of risks should be addressed in the policy, including, but not limited to:

- Data privacy
- Protection of intellectual and proprietary information
- Rules of engagement for spokespersons
- Expectations related to productivity
- Potential liabilities for misuse
- Monitoring and auditing

At the end of the day, the final policy should reflect the organiza-

tion’s line of business, culture, and risk tolerance.

Policy Implementation and Beyond

As with any policy or standard, an organization should not underestimate the time it will take for drafting, vetting, and, ultimately, approving the policy. However, the rubber will meet the road when it comes to training. An organization must engage employees at all levels of the organization. Setting the ground rules will be very important for employees who use social media on their personal time and believe they can interact with social media in the same way while at work.

Remember that employees who make ill-advised comments using e-mail will do the same using other tools. Strategies to consider for raising awareness and training could include:

- Town meetings to introduce the

social media policy, encourage questions, and provide examples as to expectations for appropriate conduct

- An internal social media site that invites employee comments and provides feedback or utilizes interactive venues to demonstrate what is acceptable social media behavior in the workplace (Making good use of these tools helps employees see the leadership team “walks the talk” and uses a medium younger employees can relate to.)
- Training modules specifically created for employees who are more

... the final [social media] policy should reflect the organization’s line of business, culture, and risk tolerance.

likely to use social media on a regular basis (e.g., sales, marketing, and public relations personnel)

- Awareness materials created to help employees connect the dots between social media and other organizational compliance standards and policies

RIM professionals can and should play a key role in developing and implementing social media policies. Drawing on experiences and relationships, they can facilitate a successful social media policy implementation strategy.

Paula Harris, CRM, has nearly 20 years of records management experience working with a variety of organizations. She is currently the director for global records and information management for Georgia-Pacific. Harris is an active member of the Publications Editorial Board for ARMA International. She can be contacted at pharris@gapac.com.



IT's Role

in Managing Social Media

Patrick Cunningham, CRM, FAI

Tweets on Twitter, statuses on Facebook, and videos on YouTube ... social media's impact is significant upon the enterprise. IT sits in the middle of the whirlwind. This article will explore:

- The role of IT in securing and making available the social media galaxy
- Social media when made available as an enterprise's official presence, when utilized personally by employees or customers, and when utilized within the enterprise

As of January 10, 2011:

- Facebook had more than 500 million active users emphasizing that its draw is hard to resist for most enterprises.
- Twitter claimed 175 million users and 95 million daily tweets.
- YouTube had 2 billion views a day.

These statistics represent the thousand-pound gorillas of social media sites. Many organizations are placing significant value upon these

types of social media sites as a means to connect to customers and deliver content to employees and shareholders. Most are gravitating to these major players, placing their own presence in the social media world with the largest communities. Some organizations find social media so valuable, they bring variants of the more popular sites into their own intranets.

The shift of social media to the mainstream means that IT must adapt. In the past, social media sites were often blocked as attractive nuisances and time wasters, but for the many enterprises now embracing social media for marketing purposes and for distribution of content, access to these sites must be provided to employees. This creates two major concerns for IT: 1) protecting the organization from external and internal information security threats and 2) controlling bandwidth usage to maintain quality of service.

Providing Information Security

The role of IT, relative to information security is two-fold:

1. Defending the organization from threats outside the organization
2. Preventing the deliberate or inadvertent release of confidential information from within the organization

Protecting the organization from an external threat is a standard part of the mission of information security. The tools the organization uses to monitor threats and counter malware will generally be applied to threats originating from social media. Intrusion detection systems, antivirus software, and firewall logging can be utilized to counter any threats from social media sites.

Organizations can also utilize web filtering tools to limit or block access to social media sites or elements of those sites. Generally, mainstream social media sites have comprehensive security controls and robust security infrastructures.

However, the scale of these sites increases the threat surface and opportunities for attackers to compromise the site or elements of the site, including content and applications associated with the site.

The threat from an organization's employees is focused on the release of confidential information, although information posted by employees about themselves can be utilized by an

organization may need to utilize external resources to scan and monitor social media sites for sensitive information.

Protecting Bandwidth, Quality of Service

Some IT organizations find that the popularity of social media sites increases bandwidth demands upon enterprise networks. The demands

usage and identify new social media sites that bear watching. Some reporting will also parse a social media site's components, allowing the network manager to understand the consumption of bandwidth by the core site, games, or other media coming from the site. This can enable the network manager to make informed decisions about the impact of various elements of social media sites on network performance.

Selecting Social Media Partners

IT professionals have a role to play when the organization selects a social media platform for its official presence. For the most part, IT will look at information security considerations and likely perform a risk assessment. This review will identify potential vulnerabilities that an organization may face by partnering with a social media site.

The organization should also give consideration to how the social media partner will respond to security incidents. The organization should require the social media partner to remove inappropriate content on demand and restore the organization's content should the site be defaced or tampered with. Many social media companies are not able or willing to monitor or disclose information about users to third parties. This limits an organization's ability to conduct investigations or trace leaks.

The risk assessment should also examine the ability for an organization to reset or disable an account that posts to the social media site. That assessment should include an emergency process, as well as a comprehensive understanding of the controls in place to secure that process.

Part of the risk assessment should include a review of the social media company's records retention capabilities, particularly with a view toward when the social media site will purge content. In addition, the

... the scale of these sites increases the threat surface and opportunities for attackers to compromise the site ...

adversary to identify key employees to target with phishing or social engineering attacks. Employees can unknowingly release confidential information. It may be commonplace for them to discuss confidential information in the office and, as a result, casually post information about their work to Facebook or LinkedIn.

In 2009, several bloggers mined public profiles on the LinkedIn social networking site and pulled together a feature set for the then-unreleased Windows Mobile 7 operating system for smart phones. The feature set was based upon information that employees of several companies had posted to their profiles. In several cases, the information was not public, and one employee posted an internal code name for an unreleased product on his public profile.

Systems that monitor network traffic for keywords, product code words, or security classification phrases can assist in identifying inappropriate postings being made from within the organization to social media sites. They do not, however, protect against postings made from mobile devices or by employees not connected to the organization's network. The information security

for bandwidth are significant and potentially disruptive when employees access streaming video, audio, or online games.

A YouTube video goes viral and much of the organization immediately brings up YouTube to view the video. Network usage spikes and normal network traffic slows to a crawl. End users flood the Help Desk with complaints about "slowness." It's a perfect storm. IT managers can dread these sorts of events brought on by social media.

Most network managers have tools to limit the impact of a rush to a viral video. These can range from web caching servers (servers that maintain copies of frequently viewed web pages and page elements that can be quickly distributed from within the organization's network) to web filters that block certain media types. Other tools can throttle bandwidth demands by limiting throughput of certain types of media.

IT professionals should monitor network bandwidth consumption by employees accessing social media sites to identify trends and risks. Many firewalls and proxy servers can provide reporting that enables network managers to follow trends in

social media company should be asked to provide its subpoena response process and demonstrate how the social media company will aid an organization's litigation efforts.

In many cases, these processes have not been formalized or are not generally available to organizations that create a presence on the social media site. Where the processes exist, they are generally not subject to modification. Terms, policies, and processes are generally subject to modification when the organization pays the social media site for its presence.

Administering Social Media Presence

The organization should endeavor to follow its own policies with regard to passwords and limit the number of employees who are given access to the credentials that allow content to be placed on the social media site. That means that unique user IDs should be created for each person authorized to post content and the use of strong passwords (complex, non-dictionary strings of eight or more characters) should be mandated, regardless of the site's minimum requirements.

From time to time, the information security or internal audit function in the organization should audit the use and distribution of user IDs and passwords. When an employee with administrative access to the social media site leaves the organization, his or her unique credentials should be immediately deleted or, if the credentials are shared, the password should be changed.

Maintaining a record of the content posted or delivered to the social media site is difficult. However, some vendor companies have developed software or hardware appliances that allow the content of social media sites to be captured and archived. IT staff can aid in selecting and integrating these tools into the

IT's role is to provide guard rails to enable access without exposing the organization to unnecessary risk or disruption.

organization's technology infrastructure.

Bringing Social Media to Intranets

The popularity of public social media sites has influenced the deployment of internal social media sites at many organizations. These sites leverage the essential functionality of social media sites, while providing the opportunity for the organization to add its own branding and look and feel.

Many organizations feature microblogging sites (similar to Twitter), internal video hosting sites, and employee profiles where employees connect to other employees. These sites allow free-flowing communications, insight into other employees' skills and interests, and the ability to create networks and share information outside of more formalized channels. The IT function can develop requirements for these sites, identify vendors, and integrate these tools into existing technology infrastructure. For some organizations, these internal sites are widely used and leveraged across the entire organization. There are some risks, however.

While internal sites are often much more secure than external social media sites, the free flow of information can inappropriately expose security-classified information or spread inaccurate information across an organization more quickly than an organization can move to correct the misinformation.

The casual nature of social media may also invite issues with employee

conduct and behavior. At the same time, the speed of information flows and the ability to connect disparate areas of the organization can constitute a competitive advantage for the organization.

Providing Guard Rails

The role of IT in social media is to enable access to social media sites, recommend means to limit threats from social media sites, and assist in the administration of the organization's presence on social media sites.

Other parts of the organization can develop compliance policies, but IT's role is to provide guard rails to enable access without exposing the organization to unnecessary risk or disruption. In addition, IT can provide the tools necessary to retain a record of content on social media sites and investigate information breaches that occur via social media.

Patrick Cunningham, CRM, FAI, is senior director, information governance at Motorola Inc. Cunningham joined Motorola in 2007. His professional experience includes more than 20 years of records and information experience. Cunningham has served on the boards of ARMA International and the ARMA International Educational Foundation. He is a frequent speaker on various RIM topics and has authored several articles on technology topics for ARMA International, including an article that won ARMA International's Britt Literary Award in 2009. He can be contacted at patrick.cunningham@motorolasolutions.com.

IS YOUR BUDGET BOXED IN BY OFF-SITE STORAGE FEES?



SAVE UP TO
68%

ON-SITE WITH BANKERS BOX®

You can use on-site solutions for a fraction of the cost of off-site storage

On-site solutions save time by giving you instant file access

On-site storage reduces handling of your records and increases control of who has access to your files

Visit www.fellowes.com/save to Learn How to Save with Bankers Box® On-Site Solutions.

QUALITY OFFICE PRODUCTS SINCE 1917





Mitigating Legal Risks

of Using Social Media

Sharon D. Nelson, Esq., and John W. Simek

During a 2010 conference, counsel from Coca-Cola and Sprint enthusiastically referred to their “social media ninjas,” or those employees who are charged with using social media on the organization’s behalf. They were clearly true believers who have invested a lot in social media and, more importantly, are enjoying the payoff.

The rise of social media has provided incredible marketing, recruiting, and customer relations benefits. Tech-savvy employers utilize these technologies to advertise employment opportunities and connect with existing and potential customers. The allure of riches to be gleaned from social media has been so great that many organizations have jumped on the bandwagon without considering

where they want to go and how they should get there. They see the riches, but often fail to evaluate the risks.

Identifying Social Media Risks

The downside of social media: its use may give rise to potential legal liability and adversely affect brand or organization reputation. Thoughtful use of social media and the development of a coherent and practical social media policy are essential. Organizations need to bring together management, IT, human resources, business development, records management, and legal personnel to formulate a good policy, one that will limit risks and maximize benefits.

Adverse Publicity

A few years ago, musician Dave Carroll looked out the window of a

United Airlines plane to see baggage handlers allegedly tossing his \$3,500 Taylor guitar like a basketball. It arrived at his destination in two pieces. Conventional attempts to resolve the matter failed, so he created a catchy little tune called “United Breaks Guitars” and posted it on YouTube. More than 8 million hits later, and with the media all over the story, United buckled and donated \$3,000, at Carroll’s suggestion, to the Thelonius Monk Institute of Jazz.

United, badly stung by adverse publicity, began to get the message and set about learning how to leverage social media. Now, United routinely responds to social media complaints. Individuals have “tweeted” about a problem only to be contacted by United to resolve the matter. United clearly took to heart the U.S.

Marine Corps unofficial mantra: “Improvise, Adapt, and Overcome.”

Most organizations that embrace social media do so because these sites provide a closer, more personal interaction between the marketer and the target audience. This allows customers to feel more involved in the community of customers, while also giving companies better and faster customer opinions about a particular product or service. But, as the Dave Carroll story shows, customers can employ social media to air their

grievances, which often demands a response to quiet the waters.

Undisclosed Endorsee Connections

In addition, the FTC has released its endorsement and testimonial guidelines applicable to social media advertisements entitled “Guides Concerning the Use of Endorsements and Testimonials in Advertising.” Specifically, the guidelines provide that if there is any material connection between an organization and an

employer can and should verify a potential applicant’s employment history if it is readily available on a social networking site (e.g., LinkedIn), and any information that implicates unlawful conduct can serve as the basis for retracting a job offer or terminating an employee.

Aside from that, employers must tread carefully. Employers who screen applicants using these sites may be providing a rejected applicant with a basis for claiming that the employer’s decision was based on a protected characteristic (e.g., race, gender, and sexual orientation) that was readily apparent on the applicant’s profile. Although the applicant will have to prove the employer’s decision was based upon the characteristic in making the adverse employment decision, an admission that the employer examined the individual’s social media pages can make it easier for the complaint to survive a summary judgment motion and embroil the employer in costly litigation.

Violating the Fair Credit Reporting Act (FCRA) – In addition, employers that choose to screen blogs and social networking profiles must also comply with the FCRA, which requires an applicant’s (or employee’s) consent before an employer may engage a consumer reporting agency to produce a consumer report on that individual. Although the FCRA permits the use of consumer reports that contain information gleaned from social media, the employer must disclose that the information resulted in the adverse employment decision.

Violating Expectation of Privacy – Employers who access an employee’s social media sites, especially those with privacy settings, will likely face allegations that they visited these sites without express permission (i.e., the employer violated the employee’s expectation of privacy). Organizations do not have unfettered access to these accounts;

Damaging content can spread globally in hours before someone notices and removes it.

grievances, which often demands a response to quiet the waters.

Misleading Advertising

Another risk comes from the Federal Trade Commission’s (FTC) Act (15 U.S.C § 41 et seq., 1914) on unfair or deceptive acts or practices, which broadly covers advertising claims, marketing and promotional activities, and sales practices. Just like traditional advertising, this means all social media ads must be truthful, not misleading; advertisers must have evidence to back up their claims, and advertisements cannot be unfair.

Unvetted Postings

The informal nature of social media advertising and the fact that it is not generally closely monitored can produce a higher risk of legal liability for the company. In particular, the traditional and serious vetting processes for advertising and press releases are almost nonexistent because social media marketing is a daily torrent. Moreover, blog posts and comments on online communities are usually not screened before they appear. Dama-

ging content can spread globally in hours before someone notices and removes it.

online poster, the connection must be disclosed by the individual. Hence, an employee who favorably blogs or comments on the organization or its products may be deemed an endorser under the guidelines, thereby subject to the disclosure guidelines. Failure to disclose the connection can, in some circumstances, result in the imposition of liability on the company regardless of whether the company approved (or even knew of) the post.

Illegal Employment Practices

The use of social media by employees for business- and non-business-related purposes is an area fraught with legal pitfalls and requires careful consideration on the part of management and legal counsel. Employers have always done some background checking on prospective employees; however, while social media sites afford more background information than ever, their use may result in unwitting violations of privacy, equal protection, or fair financial practice statutes.

Discriminating Against a Protected Characteristic – Certainly, an

any enhanced privacy controls must be scrupulously respected. These controls will not only increase an employee's common law claim to privacy, but attempting to circumvent these controls can violate federal law in addition to the social networking site's terms of service.

Making Unauthorized Access – Specifically, a federal cause of action might exist under the Computer Fraud and Abuse Act, in which an employer, in accessing an employer's social media profiles, exceeds authorized

employee if they discover information pertaining to questionable, but legal, off-duty conduct on an employee's social media page.

Some of these provisions do contain an exception for material conflicts of interest, such that an employer could lawfully take action if the employee's conduct harms the employer, even if the conduct is otherwise lawful. Courts, however, have yet to provide clear-cut legal guidelines on this issue:

- In *State v. Wal-Mart Stores*, two

negative comments about her supervisor to her Facebook page, which drew many supportive comments from some of her co-workers, violated the NLRA. Specifically, the NLRB argued that the employee's actions were protected and that the organization's policy prohibiting disparaging comments was itself a violation of the NLRA. Ultimately, the employer reached a settlement with the NLRB and agreed to rewrite its social media policy prohibiting negative remarks in cyberspace. As a settlement, the outcome is not binding on employers, but it should certainly suggest caution. This case provides a clear statement that social media policies are going to be a new focus of NLRB enforcement actions.

... social media policies are going to be a new focus of NLRB enforcement actions.

access in obtaining data from the website's computer system, and the Electronic Communications Privacy Act, in which an employer engages in unauthorized access of electronically stored data or electronic communications.

Violating State and Federal Laws – Even if an organization lawfully accesses information on an employee's social media pages, some of that information might be afforded protection under various state and federal laws. For instance, certain communications are protected because they constitute protected complaints of discrimination or whistle blowing. For example, comments about compensation or workplace safety could fall under the protections of the National Labor Relations Act (NLRA).

Moreover, certain states, such as California, Colorado, and New York, have enacted "lifestyle" laws that prohibit an employer from taking adverse employee actions based on lawful, off-work conduct. In these states, companies cannot fire or discipline an

employees were terminated by Wal-Mart for dating while one of the employees was married to another person. In upholding the organization's decision to terminate the employees, the court held that dating was not considered to be a "recreational activity" and, therefore, was not protected by New York's lifestyle discrimination statute. Shortly thereafter, the New York courts took a more expansive view of "recreational activities" protected under the statute.

- In *Pasch v. Katz Media Corp.*, the court expanded the definition of recreational activity to include cohabitation. The court has since returned to a less expansive definition of recreational activity, choosing instead to follow the holding in the *Wal-Mart* case.
- Recently, the National Labor Relations Board (NLRB) filed a complaint against the American Medical Response, a Connecticut ambulatory service company. In the complaint, the NLRB claimed the termination of an employee for posting

Mitigating Social Media Risks

Monitor Employee Activity

Given these potential pitfalls, an organization might choose to forego monitoring employee activity on social media sites. This is a bad idea. Failing to take action on employee comments that might be considered discriminatory or harassing, especially if brought to the organization's attention, could also land the organization in hot water.

- In *Blakely v. Continental Airlines*, a female pilot filed a complaint alleging a hostile work environment and defamation against the employer airline after derogatory comments about her were posted on another pilot's electronic bulletin. The court ultimately denied the airline's motion for summary judgment as to the hostile work environment claim, holding that Continental had a duty to take effective measures to prevent the harassment when it knew, or at least had reason to know, that the conduct was occurring in a workplace-related setting.
- In *Simonetti v. Delta Air Line, Inc.*, a female flight attendant filed suit

on the basis of sexual discrimination after the airlines discovered “inappropriate” photographs of the employee in her Delta uniform posted on her blog. Simonetti claimed the airlines did not punish male flight attendants who maintained blogs containing similar content. Although the case was not adjudicated because Delta filed for bankruptcy shortly after the lawsuit was filed, it still stands as a stark reminder that failing to monitor social media activity can lead to costly lawsuits.

An organization that fails to scrupulously monitor its employees’ usage of social media risks missing a post that reveals the organization’s proprietary or confidential information. Without question, social media has dramatically increased the possibility of sharing such information, especially since the informal nature of posting to these sites makes it very easy to inadvertently disclose too much.

A single tweet saying, for instance, that the employee has been working on a new invention for Company X could have severe repercussions. Since it’s so easy to also post photos and videos to social media sites, this means an employee could inadvertently reveal a wealth of information about the culture of the organization, who works there, what products are in use, and even details about customers.

Crowdsourcing, defined as the act of outsourcing tasks traditionally performed by an employee or contractor to an undefined, large group of people or community (a crowd) through an open call, has further compounded the problem. Crowdsourcing can make it very difficult, if not impossible, for an organization to retain any expectation of confidentiality in the work product being “crowdsourced.”

Finally, monitoring social media can prevent a few ill-advised tweets or blog postings from tarnishing an

Major Elements of a Social Media Policy

A well-crafted policy should:

1. Address all potential pitfalls in a clear and organization-specific manner and be consistent with other organization policies and procedures
2. Distinguish between business and personal use (on-the-job and off-the-job conduct)
3. Inform employees of the rules and regulations that state they will have a reduced or non-existent expectation of privacy on any of the organization-provided computers, e-mail systems, mobile devices, and telephone or voicemail systems
4. Encompass what can be said, who can say it, and the manner in which things should be said

An organization’s policy should provide a clear expectation of what an employee is permitted and forbidden to say. Addressing content that can be posted on social media sites can prevent a variety of mishaps, including:

- Preventing the inadvertent posting of confidential information and trade secrets
- Curtailing defamatory or otherwise inappropriate content
- Stopping any other unlawful or criminal information from being posted

The policy should instruct employees to:

- Avoid controversial subjects
- Use a polite and respectful tone, even when disagreeing
- Never post anything that could conceivably be construed as discrimination, harassment, or defamation

The policy should limit who has the authority to speak on the organization’s behalf. To effect such a strategy, consider:

- Banning those individuals not authorized to speak for the organization from using any of its intellectual property (e.g., logos, trademarks, and copyrights) in any manner
- Forbidding the use of the organization’s name in particular forms (e.g., username and screen name), but perhaps specifically allowing it as part of the employee’s profile so long as the information remains current

The essence of a good policy is simple: “Don’t be stupid.” While many more words are perhaps advisable for the sake of clarity, that’s what it all boils down to.

organization’s image. Domino’s learned firsthand the power of social media after two of its employees posted videos of themselves doing a number of unspeakable things to the pizzas they were making. The resulting avalanche of views was a public relations nightmare.

When searching for Dominos, the YouTube video popped up prominently, only compounding the problem. Making matters worse, Domino’s waited nearly two days to respond, by which time close to 1 million people had already viewed the videos, and blogs, forums, and Twitter were

inundated with discussions of the incident. Even though the employees were fired and an apology was issued, the damage to the organization was done. Consumer perception of the brand soured.

Similarly, companies that maintain a Facebook page can learn from the Nestlé incident in which a Nestlé employee posted a comment on the organization's Facebook page requesting that those who comment-

mination. In addition, employees should be required to attend regular training and meetings to ensure they remain current on any new changes in the policy, as well as new developments regarding changes in the social media sites themselves. If changes in the policy are required, it might be a good idea to send an organization-wide e-mail highlighting the changes and announcing any upcoming training sessions.

has been the experience of Sprint and Coca-Cola, whose ardent embrace of social media was mentioned earlier, that those who abuse social media are generally known to their colleagues. Nevertheless, many employers are aghast when they are shown data gathered with specialized hardware and software tracking employee usage of social media.

Social media sings a sweet siren song indeed, and yet it can morph in an instant to Pandora's Box.

ed on the page not use altered versions of Nestlé's logo for their profile pictures, saying their comments would be deleted. Site visitors reacted poorly. Unfortunately, the employee lost his cool and went on the offensive, responding to individual posters in a tone that was at times sarcastic or antagonistic. The resulting ruckus caused Nestlé a major headache as it tried to engage in damage control.

Develop Clear Policy on Social Media Use

Most of the social media risks can be minimized by carefully crafting a social media policy coupled with implementing a few technological safeguards. There is no need to reinvent the wheel; IBM and Coca-Cola have posted their social media policies online, which can provide a good starting point. See the sidebar on page HT11 for the major elements.

Provide Strong Consequences, Make Them Clear

Any good policy must have teeth. There must be a clear statement providing that any misuse of social media by employees can be grounds for discipline, up to and including ter-

Impose Technology Controls

Organizations should also consider whether or not to impose technological controls on social media usage. The key words are "try to impose" because the advent of smartphones has made control difficult, if not impossible, to achieve. Even if the organization-owned smartphones are controlled, many employees have personal smartphones, as well. Organizations have learned, to their chagrin, that their employees are adept at making end-runs around technological barriers.

Many organizations do forbid the use of social media at work, generally using hardware or software to block common social media sites. For those organization-owned smartphones that are sophisticated enough for advanced security measures to be taken, access to social media sites can also be banned.

However, most organizations are embracing the use of social media at least to some extent. Even where social media use is permitted, many companies will use hardware or software to monitor usage. Without question, social media usage can be the mother of all productivity drains. It

Create a Media Czar Position

Finally, depending on the size of the organization and the nature of its social media use, it may need a social media czar to oversee both an ever-changing social media landscape and the technology available to use and monitor it. Organizations are now beginning to create such positions.

Balance Social Media Potential Against Risks

Facebook, Twitter, YouTube, and their social media brethren have been in use for only a few years, and yet they have revolutionized business marketing and customer relations. This is very much a revolution in progress, and each year brings new technologies, new regulatory requirements, and new court decisions important to individuals who manage social media usage within their organization.

Social media sings a sweet siren song indeed, and yet it can morph in an instant into Pandora's Box. Success with social media, while limiting risk, requires constant vigilance.

Sharon D. Nelson, Esq., is president and John W. Simek is vice president of Sensei Enterprises Inc., a legal technology, computer forensics, and information security firm based in Fairfax, Va. Special thanks goes to Sensei paralegal Jason Foltin for his excellent research on this topic. Nelson can be contacted at snelson@senseient.com. Simek can be contacted at jsimek@senseient.com.

Classify...Dispose...Migrate

Classify – Millions of Shared Drive Files quickly and accurately.

- ✓ Advanced technology
- ✓ Full quality assurance
- ✓ Business Transformation

Dispose – Compliant disposition processing for shared drive files.

- ✓ Leverage your Retention Schedules for improved business productivity, reduced risk and storage savings

Migrate – High value content to ECM where it belongs.

- ✓ Remove the risk of migration through content classification and metadata association



Perram

info@perramcorp.com
1.877.213.7431 ext.222

A chain is only as
strong

as its
weakest link

With Autonomy Information
Compliance, there are no weak links

Autonomy seamlessly links information across the entire enterprise using a single, powerful platform. With the ability to manage over 25 petabytes of data and understand the meaning of complex information, organizations can archive sensitive information and apply the correct risk management, security and compliance policies to data of any kind in real time including social media interactions, audio and video, based on an understanding of the actual content. This continuous chain provides absolute control and visibility to manage the inherent risk in business information according to corporate, regulatory and legislative rules.

Leverage the strength of the Autonomy chain:

- 86 of the Fortune 100 use Autonomy Technology
- De Facto Standard for Global Enterprises, Securities Firms, and Regulators
- Only Vendor to Lead in Email Archiving, eDiscovery and Enterprise Search
- Analyzes and enforces policy against 400 million interactions each month
- Manages world's Largest Private Cloud

Build a chain that works for you—onsite or in the cloud:

www.protect.autonomy.com/compliance

