The Sedona Conference Journal

Volume 14 2013

The Sedona Conference Primer on Social Media

The Sedona Conference

Recommended Citation: The Sedona Conference, *Primer on Social Media*, 14 SEDONA CONF. J. 191 (2013).

For this and additional publications see:
https://thesedonaconference.org/publications

THE SEDONA CONFERENCE® PRIMER ON SOCIAL MEDIA*

A Project of The Sedona Conference® Working Group on Electronic Document Retention & Production (WG1)

Author:
The Sedona Conference®

Senior Editors:
Alitia Faccone
Ronni D. Solomon

Contributing Editors:
Denise E. Backhouse
Michelle Greer Galloway
Tim Gordon

Contributors:
Craig Carpenter
Deborah Juhnke
Edwin E. Lee
W. Lawrence Wescott

WG1 Steering Committee Liaison:
Jonathan M. Redgrave

We thank all of our Working Group Series℠ Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series℠ publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference® Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong nor do they necessarily represent official positions of The Sedona Conference®.

PREFACE

Welcome to *The Sedona Conference® Primer on Social Media*, a publication in The Sedona Conference Working Group Series℠ ("WGS℠").

On behalf of The Sedona Conference®, I want to thank the drafting team and all WG1 members whose comments contributed to this Primer and for all of their efforts to make this work product as helpful as possible. I especially want to acknowledge the contributions made by Ronni Solomon and Alitia Faccone, who assumed the leading roles in editing the Primer, and WG1 Steering Committee Liaison Jonathan Redgrave, who brought the Primer over the finish line. And on behalf of the Drafting Committee, I'd like to thank 2012-13 WG1 Steering Committee Chair Conor Crowley for his special contributions, guidance, and commentary on this Primer.

Unlike many of the previous publications in this Series, this is not entitled a "Commentary," nor does it present any formal "Principles," although it contains plenty of practical guidance for attorneys, judges, and parties. This is called a "Primer" because the goal is to provide primary instruction to the bar and bench in the basics of social media and the law, from definitions, to the use of social media in business, to the discovery of social media in litigation, to professional responsibilities lawyers have in relation to their own use of social media. This is a fast-developing and fast-changing area of technical, social, and legal development, and any consensus-based commentary or set of principles that claims to advance the law in this area may be doomed to obsolescence as soon as it is announced on Twitter. However, we hope that this Primer represents a positive first step in grounding the dialogue leading to consensus on moving the law forward in the reasoned and just way.

We hope our efforts will be of immediate and practical assistance to lawyers, judges, database management professionals, and others involved in the legal system. As with all of our WGS℠ publications, we anticipate that developments in the law and technology will necessitate revisions and updates of this Primer. Your comments and suggestions for future editions are welcome. If you wish to submit any further comments, please visit our website at www.thesedonaconference.org and join the online discussion forums, or email us at info@sedonaconference.org.

Kenneth J. Withers
Director of Judicial Education
The Sedona Conference®
October 2012

TABLE OF CONTENTS

INTRODUCTION

Hundreds of millions of individuals now use social media to communicate and to build online communities.[1] And these users are not only the young. A Pew Research paper issued in August 2010 notes that "[s]ocial networking use among Internet users ages 50 and older has nearly doubled – from 22% to 42% over the past year," and "[h]alf (47%) of Internet users ages 50-64 and one in four (26%) users ages 65 and older now use social networking sites."[2]

Social media is also increasingly important for business organizations and the legal community – the former largely because of their marketing potential, and the latter as yet another source of information to be regulated, managed, and ultimately preserved and produced during investigations or litigation. Twenty-two percent of Fortune 500 companies now have a public-facing blog that has received at least one post in the last 12 months.[3] And in a sign of the times, Pepsi dropped a long-running Super Bowl TV advertising campaign in favor of a $20 million expenditure on a social media campaign.[4]

Despite, or perhaps because of, the ubiquity of social media, the term defies easy definition. Given the variety and fluidity of forms and formats, it may be more helpful to focus on the most common features of social media content. Social media typically features content that is:

Shared (the content is made available to others)
Interactive (participants are often both suppliers and users of related content)
Internet-based (the content is accessed via the World Wide Web)
Personal (the content usually represents personal commentary or art, or solicits such input)
Informal (the content is typically conversational, candid, unstructured, and unedited)

Social media formats may include text, graphics, audio, or video, with a range exemplified by such familiar social media sites such as LinkedIn, Twitter, Wikipedia, Myspace, Facebook, Flickr, BlogTalkRadio, and YouTube.

Organizations should be sensitive to the inherent risks and rewards of social media and should develop a clearly defined strategy that takes into account the four typical ways in which they can be used:

- A company may use social media to shape a formal business presence based on a clear corporate objective;

- Employees may use social media to pursue legitimate business goals that may or may not be officially authorized;

1 Alyse Speyer, 12 Amazing Social Media Statistics, January 28, 2011, http://www.blogher.com/12-amazing-social-media-statistics (last visited Apr. 3, 2012).
2 Mary Madden, Older Adults and Social Media, August 27, 2010, http://www.pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx (last visited Apr. 3, 2012).
3 Nora Ganim Barnes, Ph.D. & Eric Mattson, *The Fortune 500 and Social Media: A Longitudinal Study of Blogging and Twitter Usage by America's Largest Companies*, February, 2010, http://www.umassd.edu/cmr/studiesandresearch/thefortune500andsocialmedia2010study (last visited Apr. 3, 2012).
4 Jennifer Preston, Pepsi Bets on Local Grants, Not the Super Bowl, January 30, 2011, http://www.nytimes.com/2011/01/31/business/media/31pepsi.html (last visited Apr. 3, 2012).

- Employees may engage in personal use of social media on company property, perhaps on their own time; and

- Third parties may use social media to comment on a particular company, product, or service.

Identifying the ways in which social media is used, and understanding the typical rights or obligations related to their content, are essential steps in shaping a sensible social media policy.

Electronic discovery issues in litigation are a particular concern for organizations as the volume of data continues to grow and the costs of preservation, collection, review, and production remain high even as they decrease on a per-unit basis. Lawyers are now counseling clients in many cases to take the same preservation steps for various social media data as for other electronically stored information. Because of the complex data management and ownership issues inherent in social media, its preservation presents some of the most significant challenges in the e-discovery space.

To address these challenges, organizations should consider taking a practical approach to meeting their legal obligations by identifying overall objectives, setting clear policies, training employees, and monitoring the impact of social networking on their operations.

Toward that end, this Primer provides best practice guidance on the corporate use and management of social media, as well as their preservation, collection, and production in the form of electronically stored information (ESI). There are, of course, references to various types of social media in other publications by The Sedona Conference®, and, while some overlap may be inevitable, the goal here has been to limit this Primer to issues unique to social media.

PART ONE – ORGANIZATIONAL ISSUES

I. Use of Social Media in Business: Benefits and Risks

Social media allows businesses to extend their reach and enhance their collaborative efforts by connecting large communities with related interests. And because social media deliver nearly real-time communications from a virtually unlimited number of individuals scattered across the Internet, businesses can use social media for diverse purposes. For example, product forums can facilitate communication among customers to help them resolve their own issues. Customer complaints and other threats to corporate brands can be quickly identified and mitigated. Productivity can be enhanced by allowing employees to access time-sensitive or topical information created by experts.

Social media can also present risks, if, for example, employees spend company time accessing social media sites unrelated to the business or if they disclose confidential or proprietary data.

Before organizations adopt and use social media, they should balance the business benefits with the inherent risks of this powerful communication tool.

A. Benefits

1. Enhanced Collaboration

Social media tools provide organizations with a flexible environment in which informal interactions among a broad group of customers and business partners can be quickly and cost-effectively facilitated. These tools can foster collaboration and innovation by connecting individuals with similar interests and by connecting subject matter experts with a large, distributed network of potential collaborators. The resulting communities can then network further and share knowledge in real time and across organizational and geographical boundaries.

Social media allow organizations to communicate simultaneously with large groups of stakeholders, harnessing product, process and service innovations by inviting ideas from across the company's ecosystem. The speed and diversity of group feedback can accelerate problem solving, which in turn can lead to better and more timely solutions. Social media can also enhance the ability of organizations to capture and share institutional knowledge and to rapidly deliver information to the people who need it.

2. Improved Business Relationship

Social media can foster partner and customer relationships by improving lines of communication, engaging key partners, and providing more opportunities for greater feedback from customers. By drawing on the collective talents, knowledge, and experiences of employees, customers, suppliers, and partners, an organization can improve its performance.

Organizations that engage the broader public on topics of interest to their business using social media enjoy additional opportunities to understand customer needs and may gain new insights, particularly concerning demographics and purchasing or product usage

behaviors. Social media-powered customer service options such as peer support networks and user-generated knowledge bases allow organizations to empower their customers to help themselves.

3. Increased Productivity

Social media can increase employee productivity by enabling pervasive, time-sensitive access to information; by leveraging a community of experts or technical advances to prioritize information based on relevance, usability or ease of incorporation; and by creating communities of common interest/expertise or specific centers of excellence within an organization or business environment.

B. Risks

1. Loss of Productivity

While social media can benefit organizational users, they also create significant inherent risks. The same technology that enhances employee productivity by connecting communities of interest and experts can also sap productivity when used for purposes not directly related to core business activities. Allowing access to external social networking sites increases the likelihood that employees will engage in non-work activities on company time.

2. Lack of Security

In addition to potential loss of productivity, organizations relying on social media risk disclosure of confidential data, misuse of personal data, and damage to brand and reputation. Social media often lacks certain real security controls common in more formal corporate technical environments. Even where data privacy protection exists, it is often left to the judgment of individual users to engage that protection. Such fragmented decision making can result in an inconsistent approach to the risks and rewards of social media, and can make a coherent organizational strategy difficult, if not impossible, to achieve.

3. Disclosure of Information

The casual manner in which social media users communicate can sometimes lead to sharing too much information about projects, products, or clients – either intentionally or inadvertently. Once such information is disclosed, it may be difficult or impossible to prevent further dissemination.

The advent of social media technology has transformed organizations and some employees into "publishers." Thus, organizations should now consider whether to take advantage of the coverage afforded by media liability insurance products. Traditionally, these insurance products have been utilized by publishers of content found in books, magazines, newspapers, and also by radio and television broadcasters. However, the "publication" of content on social media sites and blogs may leave organizations vulnerable to potential liabilities arising from defamation, invasion of privacy, copyright infringement, false advertising, and trade libel. Even if an organization has an insurance policy it believes may already cover such publishing, it should verify that the policy does not contain exclusions for publication of social media content.

4. Preservation of Social Media

Additionally, organizations face the risk that social media will impact litigation and e-discovery by leaving a trail of information, documents, and records that may need to be maintained for legal or regulatory purposes. However, organizations must also remain sensitive to the role third parties play in creating or maintaining social media. Because of the complex data management and ownership issues inherent in social networking, preservation of social media presents significant challenges. *See infra* Part II, §I.A. and B. With the exception of internally hosted sites, an organization may not have access to relevant content or be in privity with the social media site, which instead has a direct relationship with an employee. Finally, organizations should consider what, if any, potential liability it may face as a result of social media activity by its employees.

II. Development of a Social Media Policy

A. Exploring the Potential Benefits of Social Media Policies for Organizations

The first question any company considering a social media policy may ask is, "Do we even need a social media policy?" As the global workforce increasingly becomes a society of content producers rather than content consumers,[5] and as momentum and control of such content continues to shift from the centralized voice of an organization to the disparate voices of numerous individuals, the need for a social media policy has become increasingly clear.[6] Indeed, a quick Internet search of the phrase "social media policy" yields over 226,000,000 results. Interestingly, however, in 2009, less than 20% of organizations had social media policies in place to monitor and mitigate the potential risks associated with the use of social media.[7] And two years later – despite rapid proliferation of social media – a Poneman Institute study reported that only 35% of organizations (national and international) had a social media policy.[8] And of the 35% with such a policy, only 35% actually enforced that policy.[9] Instead, many organizations continue to address issues related to social media reactively, rather than proactively, without giving employees clear guidelines to align their social media usage with the organization's strategy, policies, and values. Or, in some cases, the issues posed by social media are mingled with general policies and guidelines involving digital communication generally without regard to unique considerations attendant to social media.

The real question is not whether an organization should have a social media policy, but rather the extent to which such a policy can (or perhaps should) effectively

---

5 Art Shaw, *The Promise of Advertising Through Social Media,* Epic Media Group, June 8, 2010, http://blogs.imediaconnection.com/blog/2010/06/08/the-promise-of-advertising-through-social-media (last visited Apr. 4, 2012) (Social media "supports the democratization of knowledge and information, and transforms people from content consumers to content producers.").

6 Sharlyn Lauby, *Should Your Company Have a Social Media Policy?* Mashable on Facebook, April 27, 2009, http://mashable.com/2009/04/27/social-media-policy/ (last visited Apr. 4, 2012).

7 Matt Leonard, *Lawsuits & PR Nightmares: Why Employees Need Social Media Guidelines,* Search Engine Journal, August 19, 2009, http://www.searchenginejournal.com/why-employees-need-social-media-guidelines/12588/ (last visited April 18, 2012). Based on a recent survey, 58% of respondents expected to manage social media e-discovery in 2011 – more than double the 27% in 2010. Dean Gonsowski, *Two Surveys Confirm Social Media eDiscovery Has Reached Tipping Point,* eDiscovery 2.0, August 2, 2011, http://www.clearwellsystems.com/e-discovery-blog/2011/08/02/two-surveys-confirm-social-media-in-ediscovery-has-reached-tipping-point/ (last visited Apr. 3, 2012). The lack of a policy will likely have implications for social media data in litigation.

8 *Social Medial Use Could Cause Security Problems for Companies,* Bitefinder Resource Center, September 30, 2011, http//www.bitdefender.com/security/social-media-use-could-cause-security-problems-for-companies.html (last visited Apr. 3, 2012).

9 *Id.* According to Larry Poneman, with respect to "the companies with the policies in place, they are not 'vigorously enforced.'"

control social media behavior or the content it generates. A rational policy should not focus on managing the use of a particular social media site, but rather on managing the people who generate or use the content. Once an organization decides how to approach the use of social media by its employees, it must then consider whether and how the policy regarding such use will regulate the business use and/or the personal use of social media by its employees.

Understandably, employers can be skeptical about granting employees unrestricted access to social media because they are concerned about lack of control. In the business-use context, permitting employees to publicly voice their unedited opinions about the organization can be risky. When people are "posting" or "tweeting," they tend to express themselves more colloquially, making statements they would not necessarily include in a more formally prepared and edited business document. In truth, organizations have always faced the risk that their employees might disparage others, release proprietary information, or expose the organization to community disapproval. However, the explosion of social media has dramatically facilitated rapid communication to a broad audience; and the freedom from responsibility that comes with anonymity, if not anticipated and properly regulated, can transform isolated errors in judgment into incidents with potentially dire organizational consequences.

For these and other reasons, many notable organizations have banned the use of some or all forms of social media in the workplace. For example, the White House, the Marine Corps, and the Green Bay Packers have all imposed prohibitions against tweeting.[10] Recent statistics reveal that 54% of companies still do not allow employees to visit social networking sites for any reason while at work.[11] However, most employers – supported by many industry experts – agree that attempting to block access to social media sites to prevent employees from talking, texting, and now tweeting, is ineffective. Further, such a policy may actually decrease productivity.[12] Any employee with an iPhone, BlackBerry, or other personal device has unfettered access to social media portals and the ability to create content at his or her fingertips.[13] Furthermore, as a recent technology white paper found, access to social media sites does not require any special hardware or software; employees can easily bypass the security guidelines and safeguards set up by the Information Technology ("IT"), human resources ("HR"), and legal departments.[14]

10 Jay Shepard, *Five Reasons Twitterers Make Better Employees*, Gruntled Employees, August 20, 2009, http://www.gruntledemployees.com/gruntled_employees/2009/08/five-reasons-twitterers-make-better-employees.html (last visited Apr. 3, 2012). Although the White House communications team is denied access to the government's Facebook postings and Twitter feeds, the "White House New Media" team has been exempted from this policy. Michael Scherer, *Obama and Twitter: White House Social Networking,* Time, http://www.time.com/time/printout/0,8816,1896482,00.html (last visited Apr. 3, 2012). In the case of the Marine Corps, the original ban put in place in April 2009 (excluding private use by Marines on personal computers outside their jobs) was revoked one year later in April 2010 when those covered by the policy were authorized to use social networking sites, user-generated content, social software, instant messaging, and discussion forums on the Marine Corps Enterprise Network. However, access remains limited to "reasonable durations and frequency" as determined by a supervisor. Cpl. Scott Schmidt, Headquarters Marine Corps, *Social media: Changing How the Marine Corps Operates,* http://www.marines.mil/unit/hqmc/Pages/SocialmediachanginghowtheMarineCorpsoperates.aspx (last visited Apr. 3, 2012).

11 J.D.Rucker, *Social Media Use at Work Yields Higher Productivity,* Soshable, Jan. 19, 2011, http://soshable.com/social-media-use-at-work-yields-higher-productivity (last visited Apr. 4, 2012). Additional statistics reveal that 19% of companies allow use for business purposes only, 16% allow for limited personal use and 10% allow unlimited personal use. *Id.*

12 *Id.*

13 This ability and access to technology has led to the phenomenon referred to as the "consumerization of IT," a trend where new information technology emerges first in the consumer market and then spreads into business organizations, resulting in the convergence of the IT and consumer electronics industries, and a shift in IT innovation from large businesses to the home. Consumerization, *from Wikipedia the Free Encyclopedia*, http://en.wikipedia.org/wiki/Consumerization (last visited Apr. 3, 2012).

14 *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, ISACA 2010. The Information Systems Audit and Control Association ("ISACA") is a global organization focused on the security of information systems. Specifically, a representative of the ISACA has recognized, "[h]istorically, organizations tried to control risk by denying access to cyberspace, but that won't work with social media. . . . Companies should embrace it, not block it. But they also need to empower their employees with knowledge to implement sound social media governance." Lance Whitney, *Study: Social-Media Use Puts Companies at Risk,* CNet News, June 8, 2010, http://news.cnet.com/8301-1023_3-20007071-93.html (last visited Apr. 3, 2012).

Given the pronounced and increasing bias in favor of social media as a means of personal communication, organizations probably cannot completely prevent its workplace usage. Conversely, while the collective wisdom is that efforts to block or deny all access to social media are unworkable, a failure to impose any restrictions at all will lead to unpalatable risks. The challenge is thus figuring out where on this continuum from toleration to restriction the organization should land.

The answer probably lies in encouraging social media use, but limiting the number and types of social networks employees can access. Indeed, a policy that discourages social media entirely may represent a risk-averse, traditional approach to communications that could easily send the wrong signal both inside and outside the organization. However, if an organization has a positive relationship with its employees, the risks are minimized and the potential benefits are great.

No matter where an organization fits along the continuum, a written policy that sets boundaries and guidelines is sound business practice. With rapid changes in technology and constant emergence of new social media outlets and other opportunities for individuals to produce and share content, structure in the form of guidelines and policies can remove some of the uncertainty employees may have regarding acceptable conduct.

Whether the policy focuses on business use, individual use, or both, or whether it authorizes multiple spokespersons or restricts access to a select few, the most significant reason for an organization to implement a written social media policy is that in this age of democratization, a well-constructed policy ensures that the organization is speaking with a unified voice.

B. Organizational Goals of a Policy

When possible, all affected stakeholders, including business heads, risk management professionals, and representatives from human resource and legal departments, should be involved in setting goals and crafting the policy, and they should all be committed to its enforcement. As with any organization-wide initiative, there will likely be varying levels of participation and disagreements about the best final product; but compliance is more likely when all stakeholders have a voice. An inclusive approach will also help to reduce the risks of fragmented decision making and the adoption by different business units within an organization of different approaches.

In order to establish the goals and purpose of a specific social media policy, a threshold decision is whether the policy's primary goal will be to regulate usage for business purposes or usage by employees for their own purposes. To decide whether business purposes should be the focus, an organization must realistically assess its organizational and work culture. For example, is the organization a start-up online retailer looking to improve its visibility and to generate sales and a following with social media marketing? Is it an established brand looking to both promote and protect its hallmark in the global, electronic marketplace? Is it an organization in a heavily regulated industry requiring rigid compliance by its employees with applicable rules and regulations?

Whatever the organization's strategic goals and whatever the intended scope of its social media policy, the policy itself should establish clear ground rules. Educating employees should also be a primary purpose, including explaining how a posting, whether

on an organization-sponsored site or an employee's personal Facebook page, could breach organizational and informational security, damage the organization's image or reputation, or even expose the organization to malware.[15]

Another fundamental goal of any social media policy should be to address the fine line between personal and professional communications involving different forms of social media. Employees need to understand where employers draw this line; but, at the same time, organizations also need to determine how the goals and purposes of its policy will intersect and affect the privacy rights of its employees,[16] i.e., how and in what manner the employer will reserve the right to monitor employee usage. Any good policy will help establish boundaries, but the policy also needs to be flexible and it should acknowledge that the personal/business demarcation will rarely support a bright-line rule.

Social media can leverage the power of the individual and harness the collective voices of an organization. A specific policy crafted to achieve that leverage can become one of the centerpieces of an organization's strategic plan.

C. Issues to Consider in Drafting a Policy

Organizations should strive to make their policies as straightforward as possible in order to facilitate understanding and compliance. In fact, some of the more workable policies are expressed as a short list of guiding principles, often with only 5-to-10 major points. In contrast, consider the school board sued by a teachers' union for an unclear and overly restrictive policy that included a 21-point bullet list of the "Liability Risks of Using Social Media."[17]

1. Style and Structure

An organization's culture should influence the form, format, and tone of its social media policy. For example, what works in an advertising agency will likely differ from what works in a large law firm. Among the issues that should be considered are the following:

- How social media have been used in the past by the organization, and the organization's plans to expand or reduce that usage;

- Whether any specific types of social media could pose a particular concern for the organization;

15 "Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior." *Wikipedia the Free Encyclopedia*, http://en.wikipedia.org/wiki/Malware (last visited Apr. 3, 2012).

16 For example, in the state of New Jersey, the right to privacy has been more broadly interpreted than under federal law. Under the New Jersey Constitution, the right of privacy takes the form of a fundamental right to personal integrity. Although the word "privacy" does not appear in the state constitution, the New Jersey Supreme Court has explicitly articulated and broadly defined a right of privacy that protects individuals from state interference on illegitimate grounds. *See* N.J. Const. art. I; Grayson Barber, *Privacy and the New Jersey Constitution,* New Jersey Lawyer Magazine, February 2002. In the 2008 decision of *State v. Reid*, the defendant was charged with computer theft and moved to suppress evidence that her Internet Service Provider (ISP) provided in response to a subpoena. The New Jersey Supreme Court "[held] that citizens have a reasonable expectation of privacy, protected by Article I, Paragraph 7, of the New Jersey Constitution, in the subscriber information they provide to Internet service providers – just as New Jersey citizens have a privacy interest in their bank records stored by banks and telephone billing records kept by phone companies." 194 N.J. 386, 389 (2008). The Court stated that while there might not have been a violation under the United States Constitution, the New Jersey Constitution provides for enhanced privacy rights that were violated in that case. *Id.* at 396-97.

17 Mathew Pellegrino, *SRPE, teacher 'de-friending' district media policy*, August 31, 2010, http://www.srpressgazette.com/articles/policy-11089-educators-new.html (last visited Apr. 3, 2012).

- How social media usage affects employee productivity;
- Whether the organization is drafting a policy in response to an incident or questionable use of social media, or instead, is proactively outlining best practices;
- Whether the organization should address industry-specific or organization-specific concerns; and
- Who will serve as the gatekeeper for adopting new social media technologies.

A short, conversational policy encouraging employee participation in certain forms of social media may be most appropriate for some organizations. Alternatively, others may benefit from a more formal, structured policy that places significant restrictions on the use of social media in the work setting. A tightly restrictive policy may be especially appropriate in regulated industries or government agencies. Soliciting input from more than one source, including legal (inside or outside counsel), information technology, records management, and business functions, will facilitate a more effective policy and a more coherent approach.

Certain elements can transform a policy from a negative, restrictive code of conduct to one that fosters a collaborative relationship while still achieving the goal of regulating behavior. These elements may include:

- Demonstrating the benefits of engaging in social media to employees;
- Focusing on what employees have the freedom to do as opposed to the restrictions being placed on them;
- Promoting responsibility and the exercise of good judgment with respect to what is published; and
- Requiring employees to take ownership of their social media communications by always stating who they are and whom they represent and by promptly correcting their mistakes.

Organizations that encourage, or even sponsor, social media use by employees when acting on behalf of the corporation for marketing or other business purposes may wish to consider separating policy language from more general guidance regarding internal protocols or permissions. In fact, an argument may be made that every social media policy should include accompanying guidelines to frame and implement the policy language. Such guidelines might address:

- The process to be followed to gain approval for use;
- The scope of topics or information that can or cannot be disseminated through social media;
- A referral process for customer issues;

- The permissibility or form of comments regarding competitors; and
- A description of specifically disallowed activities.

Another distinction may be drawn between policies designed to guide employees in their business use of social media and their personal use of social media that may impact their employer.

In all cases, clarity is essential. The policy should incorporate specific examples and should ensure high visibility by using multiple forms of publication. Publication might take the form of a notice attached to each computer log-on, a broadly disseminated written policy, employee orientation and training, or all of the above.

2. Content

An effective social media policy should address at least three key content areas: (1) employee rights and obligations; (2) monitoring guidelines; and (3) engagement processes and roles.

Two basic life lessons should drive social media policy content: *play nice* and *don't take things that don't belong to you*. Although common sense should rule, some degree of explicit instruction should still be part of any organization's social media policy. However, the longer and more verbose the policy, the less likely it is to be effective. The goal should be to include the purpose and relevant guidelines, providing employees with the necessary structure so that they are on notice regarding the rules and the reasons for them.

As with all policies that implicate the rights of employees, a sound social media policy should promote fair, even-handed treatment. Organizations would be well served, if practical, to go beyond the initial group of stakeholders and work with the employees to determine what policies would be fair and realistic given the corporate culture. This practice would also permit the organization to gain valuable information and insight regarding the current social media behavior of its employees.

3. Legal and Ethical Considerations

Policy language should first cover basic legal and ethical considerations and provide required commentary on any specific regulatory restrictions or requirements unique to a particular industry, along with a general statement requiring adherence to all federal, state, and local laws. A second policy category may cover employees' responsibility for any content they post. This category might include language about ensuring the authenticity of posted content (*e.g.,* not knowingly publishing false information); eschewing defamatory or inappropriate content; and avoiding disclosure of personal information regarding other employees, competitors, or other persons outside the organization.

An often-overlooked twist with social media concerns is its use in research, sometimes called "scraping" or "social listening." When social media content is routinely "scraped" by company employees or by third parties ("listening vendors"), guidance should be provided to them regarding ethical obligations associated with the use of such content, such as whether the terms of service of sites have been observed.

An increasing number of organizations recommend that employees who are neither company executives nor designated spokespersons utilize a disclaimer when using social media for private purposes.[18] Disclaimers, if utilized properly, can facilitate freedom of speech while at the same time providing protection for both the employer and the employee.

4. Protecting Intellectual Property

Employees may benefit from detailed instructions that define which uses of an organization's intellectual property are acceptable and which are not. For example, employees may be told whether or when they can use logos or disclose proprietary or confidential information. By informing employees about specific, potential risks to the organization created by inadvertent disclosures, an organization can help them make better decisions and think through the consequences of their actions before they act. A well-drafted policy will also help to protect third parties' intellectual property – and to mitigate the organization's risk – by requiring attribution for all quotations or references to copyrighted works used in social media communications.

5. Definitions and Relationships

Social media use by employees may be viewed as a subset of all e-communications within an organization, and therefore will share some characteristics with email, collaborative workspaces, and other internal messaging systems. Consequently, smaller organizations or those that do not actively support the use of social media may choose to include social media policy language as a component of their other policies, highlighting any unique aspects. Under this approach, a blanket statement regarding the application of the policy to all forms of online communication and conduct may be appropriate.

Alternatively, and particularly when the organization uses social media proactively, the social media policy may stand alone but should contain references to, and complement, existing policies. These references acknowledge that there will be linkages with other organizational policies, such as those regarding codes of conduct, harassment, ethics, confidentiality, e-communications, and conflicts of interest. For example, a written policy should clearly inform employees that social media will not provide them with a refuge from confidentiality and "code of conduct" obligations they owe to their employers.[19] Maintaining and even highlighting ties and links to other policies can help place a social media policy in context and reinforce the importance of compliance. In any case, however, unless the written policies are quite short, it is generally not advisable for an organization to combine all of its rules in one master policy. Employees are far less likely to read a lengthy, comprehensive code of conduct document than concise statements of specific rules. Finally, an organization's other policies should be reviewed before setting a social media policy to ensure that the policies are consistent.

D. Compliance and Enforcement

It is an obvious corollary to any policy that there should be a way to ensure its compliance. Organizations need to communicate clearly and frequently with employees

18 Best.Buy.PR, *Best Buy Social Media Policy*, Best Buy, April 13, 2011, http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492 (last visited Apr. 3, 2012) ("State that it's YOUR opinion: When commenting on the business. Unless authorized to speak on behalf of Best Buy, you must state that the views expressed are your own.").

19 Kevin H. Nalty, *Moving Beyond Compliant Social Media*, PharmExec.com, March 1, 2010, http://pharmexec.findpharma.com/pharmexec/article/articleDetail.jsp?id=661648 (last visited Apr.3, 2012).

regarding policies and procedures; and in particular, they need to establish and communicate the consequences flowing from policy violations. Training is recommended and, depending on the organization, will likely require collaboration with representatives from the IT, HR, and legal departments. Because it is impossible to anticipate or highlight every potential scenario, training should stress a common sense approach and should help employees understand the implications of conduct, especially in the realm of personal use that might not otherwise be obvious.

A more complicated issue regarding compliance and enforcement in the social media context is monitoring. For organizations that choose not to rely on the honor system, monitoring is the only way to confirm efficacy and compliance. Further, some organizations may be explicitly or effectively required to monitor by a regulatory scheme. Establishing a monitoring practice is necessary in order to review communications and content for consistency, clarity and compliance with guidelines, especially if an organization encourages employees to contribute to its social media presence through a business-use based policy. An organization that attempts to regulate the personal use of social media in the workplace may face a more onerous task, which at its most extreme would require knowledge of its employees' social media site affiliations and then the time and access to examine each of the sites individually. While monitoring is not necessarily an all-or-nothing proposition, there are several monitoring issues to consider:

- How and in what manner will monitoring take place;
- What is the breadth and the scope of the content that will be monitored;
- Who will be tasked with the responsibility to monitor;
- What are the costs associated with monitoring;
- What privacy rights of employees are implicated;[20] and
- What, if any, less intrusive means can the organization employ to regulate compliance?

Many organizations monitor compliance with "message compliance specialists" whose specific duties include ensuring that employees neither inadvertently nor intentionally violate the organization's social media policy.[21] Another option, and one that continues to become more viable and more sophisticated, is software geared specifically to monitor, control, and record posted content, at least if it passes through the corporate

20 Consider the case of *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D.N.J. Sept. 25, 2009) wherein two restaurant employees sued their former employer following their termination for posting comments critical of the company on a private, employee-only Myspace page. According to plaintiffs, the restaurant's managers gained access to the page only after they "strongarmed and threatened" a fellow employee and member of the private group to provide them with the member's email address and password. Although the jury found in favor of the defendants on common law claims for invasion of privacy, finding that the plaintiffs had no reasonable expectation of privacy in the Myspace group, the case was still decided in favor of plaintiffs finding the managers had violated the Stored Communications Act and the New Jersey Wire Tapping & Electronic Surveillance Act by intentionally accessing the Myspace page without authorization. However, the *Pietrylo* case warns organizations that in the absence of reliable evidence that an employee is engaged in malfeasance causing serious damage to the employer's interest or violating substantial company policies, any kind of policy that allows employers to access password-protected social media sites is ill-advised.

21 Marisa Peacock, *GRC Roll-up: The Impact of Social Media and Governance*, CMS Wire, March 10, 2010, http://www.cmswire.com/cms/enterprise-cms/grc-rollup-the-impact-of-social-media-and-governance-006919.php (last visited Apr. 3, 2012).

network.[22] Other options include using Google alerts and subscribing to employee Twitter feeds. Focusing on social media as simply another communication medium, rather than as part of an organizational marketing strategy, may help an organization crystallize the scope of measurement and monitoring.

No matter what level of monitoring or other means to ensure compliance it uses, an organization should establish and communicate consequences for policy violations; and then follow through when violations occur. Here again, cultural considerations will influence the tone and severity of any policy language. Clear communication is helpful, and the policy may explain what employees should do if they have questions, how they should report a violation, and what the consequences will be for failing to follow the policy.

In some cases, organizations may consider specifying that violations of social media policies, whether as a result of business or personal use, will be considered grounds for termination of employment. Consider, however, that employees must be placed on notice about such severe remedies. Best Buy uses a compliance provision that is particularly blunt:

> **Just in case you are forgetful or ignore the guidelines above, here's what could happen. You could:**
>
> - Get fired (and it's embarrassing to lose your job for something that's so easily avoided)
> - Get Best Buy in legal trouble with customers or investors
> - Cost us the ability to get and keep customers
>
> "Remember: protect the brand, protect yourself."[23]

As varied as social media tools and opportunities are, so too are the reasons an employer may have to discipline an employee. Some primary concerns include illegal web-based conduct; unsatisfactory job performance as a result of using social media while on the job; or disparaging or harassing a fellow employee, supervisor, client, or customer. Before imposing any specific discipline, organizations would be wise to consider the possible legal consequences of such disciplinary action.[24] This is particularly true when they discipline employees for what may have been protected concerted activity, or when the policy

22 *See, e.g.*, www.nextpoint.com.
23 Best.Buy.PR, *Best Buy Social Media Policy*, Best Buy, April 13, 2011, http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492 (last visited Apr. 3, 2012).
24 *Social Media in the Workplace: Managing the Risks,* Jackson Lewis, March 9, 2010, http://www.jacksonlewis.com/resources.php?NewsID=3235 (last visited Apr. 3, 2012). Some of these constraints may include: The National Labor Relations Act; protection under a whistleblower statute; or whether the employee was engaging legal off-duty activity.

language alone might interfere with employees' perceived rights.[25] Particularly in the case of public employees, the issue of restricting free speech comes into play.

Monitoring need not be limited to employee use. Certain organizations would be well advised to employ some type of monitoring protocol to protect their brands by detecting brand theft and defamatory material that might harm the brand's reputation. This monitoring can be done internally or externally through use of services and software tools developed for such purposes. For each organization considering this type of monitoring, a cost-benefit analysis is advisable.

E. Updating the Policy

Unlike many corporate policies grounded in long-standing law, regulation, or tradition, a social media policy can quickly become outdated. Consequently, attention should be paid to updating the policy on at least an annual basis.

A number of factors may influence whether policy language should be revised:

- Attention to internal social media issues as they arise. Policies are in some part reactive responses to events as they occur in an organization. Keeping track of any significant events (such as breaches of existing policy) will help inform whether an update is in order.

- Metrics/logs. If an organization is concerned with potential excessive use of social media by employees (particularly non-business uses), then a review of Internet usage logs may provide useful metrics.

- Changes in organizational use and implementation. Any strategic, tactical, or technical change to an organization's use of social media or the enforcement of an applicable policy may require a policy update. Such changes may include, for example, a new and proactive use of social media for marketing or a move to allow greater employee involvement on behalf of the organization.

- Case law survey and regulatory changes. A growing body of case law addresses social media issues. An annual review of key rulings should be

25 In *In re American Medical Response of Connecticut, Inc.*, NLRB Case No. 34-CA-12576 (October 27, 2010), employee Dawnmarie Souza was fired for posting derogatory comments on Facebook about her supervisor. After being denied her request for union representation, Souza posted her comments on Facebook, which resulted in supportive comments from co-workers. She was fired shortly thereafter. The NLRB, pursuant to its authority to safeguard employee rights and prevent unfair employer practices, filed a complaint against AMR in October 2010, alleging the company's overly broad policies violated Section 7 of the National Labor Relations Act ("NLRA"). Under Section 7, which gives employees the right "to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection," employees must be permitted to discuss the terms and conditions of their employment with co-workers and others. By terminating Souza for posting comments that drew support from co-workers, AMR had violated the NLRA. Notwithstanding the NLRB's position in the lawsuit – which settled – the NLRB's general position remains that employers are permitted to regulate employee behavior, including speech on social media web sites. In this case, the NLRB simply clarified that these generally permissible policies regulating free speech are not permissible if they interfere with employees' rights to organize labor unions and engage in concerted activities. Jessica Martinez, *NLRB v. American Medical Response: A Rare Case of Protected Employee Speech on Facebook*, Berkeley Technology Law Journal, http://btlj.org/2011/03/07/nlrb-v-american-medical-response-a-rare-case-of-protected-employee-speech-on-facebook (last visited Apr. 3, 2012). In the more recent case of *Hispanics United of Buffalo, Inc. v. Ortiz*, and the NLRB's first written decision involving social media, an administrative law judge ruled that HUB violated the NLRA when it terminated five employees for posting complaints after-hours on Facebook about their jobs, one of their managers, and some of their more challenging social service clients. According to the ALJ, "employees have a protected right to discuss matters affecting their employment amongst themselves." The judge clarified that it did not matter that the gripes were not directed at forming a union or otherwise changing employee working conditions at HUB. Applying previous decisions, he found that activity does not need to have the goal of changing working conditions to be protected.

part of every policy analysis. Similarly, for those in regulated industries, updated regulations or new interpretations of existing ones are an important consideration.

- Changes in the complexion of social media. New forms or uses for social media will inevitably evolve that will necessitate adjustments of the social media policy.

F. Examples of Specific Policies in Action

1. The Blended Approach

The social media policy promulgated by the Coca Cola Company ("CCC") provides a good illustration of an effective policy that on its face successfully incorporates the principles stated above by clearly setting forth its purpose, establishing guidelines, providing structure, and focusing on the positive aspects of the policy and the regulation of employee conduct. Consider its stated purpose, which is printed in bold in the first paragraph:

> These Online Social Media Principles have been developed to help empower our associates to participate in this new frontier of marketing and communications, represent our Company, and share the optimistic and positive spirits of our brands.[26]

Immediately thereafter, CCC lists its core values, including leadership, collaboration, integrity, accountability, passion, diversity, and quality, and then explains how these values relate to and are incorporated into the policy:

> These Online Social Media Principles are intended to outline how these values should be demonstrated in the online social media space and to guide your participation in this area, both when you are participating personally, as well as when you are acting on behalf of the Company.[27]

CCC also recognizes the relationship between traditional media and social media and makes reference to its rules for other types of communications:

> The same rules that apply to our messaging and communications in traditional media still apply in the online social media space; simply because the development and implementation of an online social media program can be fast, easy, and inexpensive doesn't mean that different rules apply.[28]

As CCC's Online Social Media Principles serve a dual function for business and individual uses, the policy provides a list of specific principles relating to each type of use in sections entitled "Our Expectations for Associates' Personal Behavior in Online Social Media," and "Our Expectations for Online Spokespeople."[29] Moreover, the policy recognizes the interplay and tension between business and personal postings:[30]

26 *Online Social Media Principles,* The Coca Cola Company, 2006-2009, http://www.thecoca-colacompany.com/socialmedia (last visited Apr. 3, 2012).
27 *Id.*
28 *Id.*
29 *Id.*
30 *Id.*

> Online, your personal and business personas are likely to intersect. The Company respects the free speech rights of all of its associates, but you must remember that customers, colleagues, and supervisors often have access to the online content you post. Keep this in mind when publishing information online that can be seen by more than friends and family, and know that information originally intended just for friends and family can be forwarded on. Remember NEVER to disclose non-public information of the Company (including confidential information), and be aware that taking public positions online that are counter to the Company's interests might cause conflict.

Notably, CCC's Online Social Media Principles are less than three pages long.

2. Regulations and Restricted Access

At the other end of the spectrum, the "Guide to the Internet for Registered Representatives" (the "Guide") by Financial Industry Regulatory Authority ("FINRA") is tied specifically to regulatory requirements and provides employees with far less freedom. The stated purpose focuses on restriction as opposed to empowerment as follows:

> FINRA has developed this page to make registered representatives (RRs) aware of the compliance requirements and potential liabilities when using the Web and electronic communications for business purposes.[31]

And the scope of the communication the Guide encompasses is broad:

> All communications with the public are subject to compliance with FINRA rules and related interpretative materials.[32]

The Guide also makes clear that Registered Representatives are not exempt from the rules and regulations when the use is personal rather than business related. Further, the Guide specifically ties certain types of information and messages found in social networking to National Association of Securities Dealers Rule 2210, which delineates the different types of electronic communications for purposes of how they are regulated:[33]

> Social networking sites such as Facebook, Twitter and LinkedIn usually have static and interactive content. Static content like a profile, background or wall information is usually considered an "advertisement." Static content is generally accessible to all visitors and usually remains posted until it is removed. As with all advertisements and sales literature as defined, a registered principal for the firm must approve all static content. Interactive content includes real-time extemporaneous online discussions with unrelated third parties, such as in a chat room. Chat room content is considered a public appearance. Similar to extemporaneous discussions by an RR at a public appearance, interactive content does not require prior principal approval but must be supervised.

31 *Guide to the Internet for Registered Representatives,* FINRA, July 12, 2010, http://www.finra.org/Industry/Issues/Advertising/p006118 (last visited Apr. 3, 2012).
32 *Id.*
33 *Id.*

For a regulatory body, the Guide does for FINRA what the Online Social Media Principles does for CCC by providing covered employees of regulated entities with unambiguous guidelines on acceptable conduct.

3. Embracing Social Media

The Zappos model can probably be characterized by a single word – participation – and it has been recognized as one of the best established, aggressive, and successful uses of social media from a marketing perspective.[34] Although its "all-employee social media free love policy"[35] is unworkable for the vast majority of organizations, certain basic tenets of the model can be applied to any organization considering how to approach a social media policy. In particular, it provides that the company culture should support employee engagement with social media, and that the company leadership should understand and support the model. The Zappos participation model specifically conforms to the company's core values:

> As we grow as a company, it has become more and more important to explicitly define the core values from which we develop our culture, our brand, and our business strategies. These are the ten core values that we live by:
>
> 1. Deliver WOW Through Service
> 2. Embrace and Drive Change
> 3. Create Fun and A Little Weirdness
> 4. Be Adventurous, Creative, and Open-Minded
> 5. Pursue Growth and Learning
> 6. Build Open and Honest Relationships With Communication
> 7. Build a Positive Team and Family Spirit
> 8. Do More With Less
> 9. Be Passionate and Determined
> 10. Be Humble[36]

The examples of CCC, FINRA and Zappos demonstrate the wide range of social media policies used by organizations. There is no single policy that will be appropriate in all situations because policies will vary based on an organization's goals and values.

III. Privacy and User Expectations

A. A Privacy Overview

At first blush, the concept of privacy in connection with an organization's use of social media may appear contradictory since social media exist precisely to distribute information among many people. Some may even view social media as a form of public broadcasting.[37] For example, celebrity users of Twitter can have millions of followers. *See*

34 Brian Chappell, *Zappos: Social Media Marketing Example #26,* Ignite Social Media, February 4, 2010, http://www.ignitesocialmedia.com/social-media-examples/zappos-social-media-example (last visited Apr. 3, 2012).

35 *Grow Practical Marketing Solutions*, January 24, 2010, http://www.businessesgrow.com/2010/01/24/it-worked-for-zappos-it-probably-wont-work-for-you (last visited Apr. 5, 2012).

36 *Zappos Family Core Values*, Part of the Zappos Family, 1999-2010, http://about.zappos.com/our-unique-culture/zappos-core-values (last visited Apr. 3, 2012).

37 A natural question that flows from this phenomenon is whether social media is legally transforming private citizens into public figures for purposes of privacy laws, but such a concept is not within the scope of this Primer.

infra IV.A.2. However, many users of social media utilize the applications for communicating among select groups of friends or individuals both in and out of the workplace. It is in this context that users of social media may have, or believe they are entitled to, an expectation of privacy in their personal communications even if they are initiated in the workplace. *See supra* II.B. It is this dichotomy between the personal and public nature of these communications that makes privacy a difficult issue for many organizations, not only for employees but also for third parties communicating with employees. *See infra* Part II, V. It is from this blurred vantage point that courts are now carefully considering the issues and beginning to provide some guidance.

1. *City of Ontario v. Quon*

In 2010, the Supreme Court commented on the challenges of applying the law of privacy to the broader context of electronic communications in *City of Ontario v. Quon*.[38] *Quon* involved the privacy interest of a government employee in text messages he sent through his government-issued pager. Declining to set precedent on broader employee privacy rights issues, the Court observed that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[39] Of concern are rapid changes in the technology itself as well as the impact of technology on societal norms.[40] For example:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.[41]

The Court's comments here are directed towards hardware; nevertheless, they could be applied as well to software applications such as social media. Applications such as Facebook are so widespread that they could well be considered "pervasive" under the Court's analysis above, and therefore "necessary instruments for self-expression," that increase the expectation of privacy.[42] On the other hand, the increasing popularity of economical mobile devices that access the Internet may reduce the expectation of privacy, as employees might reasonably be expected to buy their own personal devices.

Quon involved Fourth Amendment issues of governmental searches. Furthermore, the plaintiff's status as a law enforcement official clearly impacted his privacy expectations. However, the Court's comments about the employer's desire to ensure that the employee was using the company-provided equipment for work rather than for personal use has relevance to privacy expectations.

38 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010).
39 177 L.Ed. 2d at 227.
40 *Id.*
41 *Id.*
42 As of March 5, 2012, Facebook had 812,145,160 users, 155,701,780 of them in the United States. http://www.checkfacebook.com.

2. Employee Privacy Interests in Social Media Usage from Email Cases

Several courts have ruled on the privacy interest of employees who use company equipment for personal email communications. In *Stengart v. Loving Care Agency, Inc.*,[43] a company's retrieval of messages from a workplace laptop computer used by an employee to access her private, password-protected web-based email account was found to violate the employee's expectation of privacy. Although the company argued that its policy permitted it to review email retrieved from company equipment,[44] the court found that the policy permitted occasional personal use and did not address use of personal, web-based accounts.[45] Under these circumstances, the court found that the steps taken by the plaintiff to secure her account created a reasonable expectation of privacy when communicating with her attorney and that these communications were privileged.[46]

In contrast, other courts have found that employees did not have a privacy interest in personal email exchanged using company equipment. In *Holmes v. Petrovich Development Co., LLC,*[47] the California Court of Appeal found that the plaintiff had no expectation of privacy when sending emails to her attorney using her employer's business email system.[48] Significantly, the court based its holding on the policy the employer had in place and the plaintiff's knowledge of that policy. The court distinguished cases like *Stengart* and *Quon*, which were cited by plaintiff. Specifically, the court found that no expectation of privacy existed here because:

> Holmes used a computer of defendant company to send the emails even though: (1) she had been told of the company's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal email, (2) she had been warned that the company would monitor its computers for compliance with this company policy and thus might "inspect all files and messages ... at any time," and (3) she had been explicitly advised that employees using company computers to create or maintain personal information or messages "have no right of privacy with respect to that information or message."[49]

The court clearly enunciated its rationale:

> [T]he emails sent via company computer under the circumstances of this case were akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him.[50]

43 201 N.J. 300, 990 A.2d 650 (2010).
44 The policy provided that the company could review "all matters on the company's media systems and services at any time," and "all e-mails, Internet communications and computer files were property of the company."
45 201 N.J. at 314-15, 990 A.2d at 659.
46 The court cited a combination of the facts in finding that she had a reasonable expectation of privacy, including that she did not store the password on her computer, and the confidential nature of the content of the e-mails, involving privileged communications with her attorney regarding her employment discrimination lawsuit against the company. 201 N.J. at 321-22, 990 A.2d at 663.
47 191 Cal.App.4th 1047 (Jan. 13, 2011).
48 *Id.* at 48-49; *accord Scott v. Beth Israel Med. Ctr., Inc.*, 2007 WL 3053351 (N.Y.Supp. Oct. 17, 2007); *see also, e.g., In re The Reserve Fund Sec. and Derivative Litig.*, 2011 WL 2039758 (S.D.N.Y. May 23, 2011) (applying four-point test from *In re Asia Global Crossing. Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005) and holding that because there was no reasonable expectation of privacy the marital communications privilege did not apply to e-mail sent using company email system).
49 *Id.* at 2.
50 *Id.* at 3.

The court concluded that because the plaintiff did not communicate in confidence, the communications were not privileged. One distinction between the cases appears to be that in *Stengart*, the employee took steps to maintain the privilege by sending the communications via her own personal email account even though she used her employer's equipment. However, in both cases, the employers argued that the policy in question permitted the use of the emails at trial. While it is unclear how the *Holmes* court would have ruled had the employee sent the communication through a personal email account, it is apparent from *Holmes* that the cloak of potential privilege may not be enough to protect communications in the face of a clearly delineated, specific corporate policy.

B. Privacy and Social Media: Expectation is Becoming Unreasonable

As the case law continues to develop in the area of social media and privacy, the trend appears to be that courts will not recognize or protect privacy interests of those who voluntarily engage in social media communications. Although initial cases addressing this issue arise in the context of labor and employment, family law, and personal injury matters, where unique considerations broadly implicate the sort of information found on social media sites, the opinions indicate that, in the future, social media and privacy could likely become mutually exclusive concepts in the law.

As the cases below indicate, courts appear to be more willing to allow discovery not only of publicly available profiles and wall postings but also of information that the user has attempted to protect using a site's privacy options.[51] Such decisions will ultimately have repercussions in the organizational context as well.

1. *EEOC v. Simply Storage Management, LLC*

In *EEOC v. Simply Storage Management, LLC,*[52] defendants sought discovery of the plaintiffs' Facebook and Myspace content to assess plaintiffs' claims of emotional distress resulting from alleged sexual harassment. The court permitted defendants to obtain content reflecting the plaintiffs' emotional states,[53] over the EEOC's objections of relevance and that such disclosures would embarrass the plaintiffs. The court noted that the privacy settings on the social media sites were not a basis for shielding the content from discovery, "[a]lthough privacy concerns may be germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose in the litigation."[54] The court observed that an appropriate protective order would address plaintiffs' privacy concerns.

2. *Romano v. Steelcase, Inc.*

In *Romano v. Steelcase, Inc.*,[55] a personal injury action, defendants sought access to the plaintiff's current and historical Facebook and Myspace accounts, including all deleted pages and related information, which may have contained information inconsistent with

51 *McMillen v. Hummingbird Speedway, Inc.,* No. 113-2010 CD (Pa. C.P. Jefferson Sept. 29, 2010) (requiring plaintiff to provide user name and password of his Facebook and Myspace accounts to opponent's attorneys over objection that the private portions of the sites were confidential); *Largent v. Reed*, No. 2009-1823, 2011 WL 5632688 (Pa. C.P. Franklin Nov. 8, 2011) (same re Facebook account credentials).

52 Case No. 1:09-cv-1223-WTL-DML, 270 F.R.D. 430 (S.D. Ind., May 11, 2010).

53 The content included "status updates, wall comments, causes joined, groups joined, activity streams, blog entries" and could also include photographs and videos, but tagged photos of the plaintiffs on the sites of third parties was less likely to be relevant. Simply Storage, supra note 41, at *14-*16.

54 *Id.* at *8.

55 Misc.3d 426 (Sup. Ct. Suffolk Co. Sept. 21, 2010).

claims she made concerning the extent and nature of her injuries. The court found that the public portions of the plaintiff's social networking sites included content that was material and necessary to the litigation, and concluded that a reasonable likelihood existed that the same would also hold true of the private portions.

The opinion was premised on two grounds: The defendant needed the information as a matter of civil procedure, and releasing the information would not violate the plaintiff's right to privacy under the Fourth Amendment.

As to discovery, the court focused on the liberal nature of the disclosure rules in New York:

> The information sought by defendant regarding Plaintiff's Facebook and Myspace accounts is both material and necessary to the defense of this action and/or could lead to admissible evidence. . . . In light of the fact that the public portions of Plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action. Preventing Defendant from accessing Plaintiff's private postings on Facebook and Myspace would be in direct contravention to the liberal disclosure policy in New York State.[56]

As to the right of privacy claimed by plaintiff, the court found that both the sites themselves and plaintiff's conduct respecting the sites precluded the existence of such a right:

> Indeed, as neither Facebook nor Myspace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy. . . . Thus, when Plaintiff created her Facebook and Myspace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as "wishful" thinking.[57]

Even before *EEOC* and *Romano* were decided, a plaintiff was ordered to produce a complete Facebook profile in *Bass v. Miss Porter's School*.[58] Defendants had sought

56 *Id.* at *7-8.

57 *Id.* at *15-*16. In the same month *Romano* was decided in New York, the Court of Common Pleas in Pennsylvania rendered a similar decision in a personal injury action. In *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD (Pa. C.P. Jefferson Sept. 29, 2010), *supra* n.50, the court also held that non-public portions of the plaintiff's Facebook and Myspace accounts were discoverable. However, rather than focus on expectation of privacy, or lack thereof, the court in *McMillen* based its holding on declining to adopt a "social network site privilege" in response to plaintiff's argument that his communications were "confidential" and "protected against disclosure." Since then several courts in Pennsylvania have granted discovery of social media data; *see, e.g., Zimmerman v. Weis Mkts., Inc.*, No. CV-09-1535, 2011 WL 2065410 (Pa. C.P. Northumberland May 19, 2011); *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371 (M.D. P. June 22, 2011); *Largent v. Reed*, No. 2009-1823, 2011 WL 5632688 (Pa. C.P. Franklin Nov. 8, 2011).

58 Civil No. 3:08cv1807 (JBA), 2009 WL 3724968 (D.Conn. Oct. 27, 2009).

documents related to plaintiff's alleged teasing and taunting in text messages and on Facebook. While the plaintiff had sought to restrict the amount of material produced, the court ordered the entire profile produced, holding that:

> Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting. Therefore, relevance of the content of Plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff's own determination of what may be "reasonably calculated to lead to the discovery of admissible evidence."[59]

The courts' treatment of the expectation of privacy is understandably different when minors are concerned.[60] Nevertheless, when central to the allegations, as demonstrated in the *EEOC*, *Romano*, and *Bass* opinions, courts have ordered the production of social media materials.

Courts have generally not allowed employers to use confidential user name and password information to access employee activity on social media sites outside of the discovery process. In *Pietrylo v. Hillstone Restaurant Group*,[61] two restaurant employees sued their former employer following their termination for posting comments critical of the company on a private, employee-only Myspace page. Plaintiffs claimed that the restaurant's managers gained access to the page only after they "strong-armed and threatened" a fellow employee and member of the private group to provide them with the member's email address and password. A jury found that the managers had violated the Stored Communications Act ("SCA") (*see infra* Part II, §III) and the New Jersey Wire Tapping & Electronic Surveillance Act by intentionally accessing the Myspace page without authorization. Interestingly, the jury found in favor of the defendants on common law claims for invasion of privacy, finding that the plaintiffs had no reasonable expectation of privacy in the Myspace group.[62] The *Pietrylo* case instructs that in the absence of reliable evidence that an employee is engaged in malfeasance causing serious damage to the employer's interest or violating substantial company policies, any attempt to obtain access to password-protected social media sites may be ill advised.

---

59 *Id.* at *3-*4. The court reviewed the material in camera before ordering the entire Facebook profile produced.

60 Cases highlighting these issues are *Beye v. Horizon*, 06-Civ.-5337, and *Foley v. Horizon*, 06-Civ.-6219, 568 F. Supp. 2d 556 (D.N.J. 2008). Parents sued on behalf of minor children over insurer's refusal to pay health benefits for anorexia or bulimia. Under then existing New Jersey law, mental illness was covered only if biologically based. Horizon Blue Cross Blue Shield sought the minor's online postings arguing that these were relevant to understanding the causes of the eating disorders, biological or emotional. The court ordered the plaintiffs to turn over the minors' writings about the eating disorders, including entries on Facebook or Myspace. *See* Mary Pat Gallagher, *Myspace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders* (Feb 1, 2008) (cases consolidated for discovery: *Beye v. Blue Cross Blue Shield of NJ,* 06 Civ. 5337 (D.N.J. 2008) and *Foley v. Horizon,* 06 Civ. 6219), available at http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005559933 (last visited Apr. 3, 2012).

61 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

62 More recently the American Civil Liberties Union requested that the Maryland Department of Public Safety and Corrections cease and desist enforcing a policy requiring that applicants for employment with the Division, as well as current employees undergoing recertification, provide the Division with all social media account user names and passwords for use in employee background checks. In a letter dated January 25, 2011, the ACLU alleged that this policy was violative, *inter alia*, of the SCA and the Maryland state equivalent (Md. Courts & Jud. Proc. Art., § 10-4A-01 *et seq*.) and also constituted an invasion of privacy "and arguably chills employee speech and due process rights protected under the First and Fourteenth Amendments to the U.S. Constitution." Letter from Deborah A. Jeon, Legal Director, American Civil Liberties Union of Maryland, to Secretary Gary D. Maynard, Maryland Department of Public Safety and Correctional Services (Jan. 25, 2011). On April 6, 2011, the Department responded by letter to the ACLU partially describing the DOC's revised policy which provided that candidates for jobs and recertification sign a form saying that they understand it is "voluntary" for them to provide access to their social media accounts during interviews. The ACLU was not persuaded, opining that it would be virtually impossible for an applicant to prove that not giving up their password was the reason they were not hired, if that were the case. According to the ACLU, what was also troublesome was that the revised policy did not take into account the interests of the Facebook "friends" whose privacy rights are ostensibly invaded by the government without their consent. Press Release, American Civil Liberties Union of Maryland, *ACLU Says Division Of Corrections' Revised Social Media Policy Remains Coercive And Violates "Friends" Privacy Rights* (Apr. 18, 2011).

C. Privacy and Social Media Policies

As discussed in greater detail in Part II of this Primer, *infra*, courts have recognized that the unique characteristics of social media can present special challenges in discovery. The *EEOC* court noted:

> [d]iscovery of [social networking sites] requires the application of basic discovery principles in a novel context. … At bottom, though, the main challenge in this case is not one unique to electronically stored information generally or to social networking sites in particular. Rather, the challenge is to define appropriately broad limits – but limits nevertheless – on the discoverability of social communications in light of a subject as amorphous as emotional and mental health, and to do so in a way that provides meaningful direction to the parties.[63]

The challenge is similar for organizations drafting social media policies and addressing the privacy considerations such policies may implicate. As an initial matter, regardless of whether the employer sponsors the use of social media by employees, it is a good idea to remind employees of the dangers associated with posting too much personal information. An employer may equally expect that employees' use of social media will not interfere with their work and may wish to include an explicit policy statement to this effect.

More particularly, policy language should contain some statement about the organization's position regarding privacy, whether personal use is permitted and to what extent; whether an employee's social media activity may be monitored and, if so, how that information may be used. This portion of the policy may also cover personal uses of social media that might impact the organization as well as business uses sanctioned for the benefit of the organization. When drafting policies that attempt to regulate employee behavior, employers should also be mindful of the *Stengart* opinion and avoid crafting a policy that may not withstand legal scrutiny. But although an employee may expect some degree of privacy in their social media communications, the nature and degree of that privacy will depend on a variety of factors, including the nature of the communication, the recipient of the communication, and the content of the communication, and, as *Holmes* demonstrates, any policy that may be in place respecting the use of social media. As with other integral parts of any social media policy, those portions dealing with privacy should be revisited regularly to keep pace with the developing law in this area.

IV. Regulatory Considerations

Social media presents a number of challenges for companies falling under the purview of regulators. On the surface, social media might appear to be like any other communication medium utilized by regulated entities; in reality, however, characteristics unique to social media set it apart from other forms of communication in several important ways. With the typical communication media – most often press releases, press interviews, and regulatory filings – there are almost always clearly identified spokespeople, media controls, and processes. With social media, in contrast, the identity of the "speaker" may be difficult to discern or verify by those viewing such commentary or by the regulated entities themselves.

---

63 *Simply Storage, supra,* 270 F.R.D. 430, at *8; *see also* Magistrate Judge Kristen L. Mix's commentary in "Discovery of Social Media," 2011 Fed. Cts. L. Rev. 5 (November 2011).

Perhaps more significantly, even speakers who are clearly identified may offer little or no information about their relationship (if any) with a regulated entity about which they communicate. Additionally, the proliferation of social media has been so rapid that both regulated entities and regulators themselves either lack well-defined policies, or have only recently issued policies governing how regulated entities should handle social media. Both the lack of well-defined and established policies and the dearth of precedent interpreting newly established policies can lead to increased uncertainty by regulators concerning control of social media, and in turn, can leave regulated entities without proper guidance.

The potential ramifications for inappropriate or illegal social media use by regulated entities are largely congruent with the compliance risks such entities already face. Examples include charges of unfair or deceptive advertising, under the jurisdiction of the U.S. Federal Trade Commission (FTC); charges of incomplete sales and marketing information, under the jurisdiction of the U.S. Food and Drug Administration (FDA); charges of disclosure of non-public information, under the jurisdiction of the U.S. Securities and Exchange Commission (SEC); and charges of making incomplete, exaggerated or misleading claims, under the jurisdiction of the U.S. Financial Industry Regulatory Authority (FINRA).

A. Sample Regulatory Guidelines

Many regulatory agencies have published social media usage guidelines for entities under their regulatory purview, including the Financial Industry Regulatory Authority ("FINRA"), the Securities and Exchange Commission ("SEC") and the Federal Trade Commission ("FTC") as well as myriad other federal, state, and local government entities. Many of these guidelines seek to address the same challenges presented by social media activity regardless of type of entity or the social media vehicle used, such as transparency, training, authorization, and disclosure:

- **Transparency**. Regulators advise employers to specify whether employees are permitted to use social media for business purposes. In theory, this practice allows consumers to better corroborate the veracity of social media communications.

- **Training**. Employers are strongly encouraged to train both authorized and unauthorized employees on the appropriate way to handle social media, the company's policies on external communication (including those using social media), and the potential risks to the entity and individual for inappropriate or illegal social media usage.

- **Authorization**. Regulated entities are encouraged to clearly identify which individuals, teams, or functional areas (if any) are authorized by the entity to utilize social media for the company's benefit. Without such clear authorization, regulated entities cannot easily establish whether inappropriate or illegal social media activity was company-sanctioned or the result of a "rogue" employee – a distinction with a huge impact on any subsequent enforcement activity or penalty.

- **Disclosure**. Social media usage by employees of regulated entities should (and in the case of the FTC must) disclose both their identity

and their relationship with the regulated entity. This allows readers of such social media communications to understand the context in which such communication is made.

1. Financial Services

FINRA has issued rules regarding social media use for securities firms in the form of FINRA Regulatory Notices 11-39 and 10-06.[64] As previously noted,[65] these rules are far more restrictive than practices applicable to non-regulated entities. Firms are required to retain records of communications related to the broker-dealer's business, including those made through social media sites. These rules may require securities firms to consider carefully the rules of a given social media site and whether available technology can record and retain content generated on that site. Regulatory requirements should also lead organizations to consider the benefits and risks of external as opposed to internal hosting of social media content.

Not only do the FINRA rules require firms to retain social media information, but the regulations also speak to policies or processes for supervising social media use and the training of employees regarding social media policies.[66]

2. Securities Markets

The SEC has reminded companies that statements made through social media outlets are corporate communications subject to the antifraud provisions of the securities laws.[67] Accordingly, companies should consider taking steps to put into place controls and procedures to monitor statements made by or on behalf of the company on these types of electronic forums.[68]

Applying its interpretation of securities laws to the use of social media, the SEC has taken action to freeze the assets of a Canadian couple who fraudulently touted penny stocks though their website, Facebook and Twitter.[69]

An additional example of the power of Twitter to impact trading was described by Dian Chu, writing in the EconForecast blog. She related how the rapper 50 Cent, who had over 3.8 million Twitter followers, tweeted about the merits of a penny stock. Subsequently, the shares in the stock jumped 290% in one day. Approximately 9.24 million shares of the stock were traded in two days. The New York Post reported that in financial documents filed by the company, its auditor raised questions about its ability as a going concern.

---

64 FINRA Notice 11-39 is available at http://www.finra.org/Industry/Regulation/Notices/2010/P124187, and FINRA Notice 10-06 is available at http://www.finra.org/industry/regulation/notices/2010/p120760 (both last visited Apr. 5, 2012). These notices are presented in Q&A format, and specifically delineate between the different topic areas covered by the Notices.

65 *See* Section II(F)(2), *supra*.

66 Seven principal points are addressed by Notice 10-06 in Q&A format: Recordkeeping responsibilities, suitability responsibilities, types of electronic forms, blogs, social networking sites, supervision of social networking, and third-party posts. *See* Spotlight on FINRA Social Media Webinar (February 12, 2010), located at http://everydaytenacity.com/asset-management-marketing/spotlight-finra-social-media-webinar-highlights (last visited Apr. 3, 2012). Notice 11-36 answers some additional questions on some of these topics, and also addresses accessing social media sites from personal devices.

67 Commission Guidance on the Use of Company Web Sites, Release Nos. 34-58288, IC-28351, effective date August 7, 2008, located at http://www.sec.gov/rules/interp/2008/34-58288.pdf (last visited Apr. 3, 2012). Speaking about interactive features of corporate web sites, the Commission noted that interactive "communications can take various forms, ranging from 'blogs' to 'interactive shareholder forums.'"

68 *Id.* at pp. 40-41.

69 *SEC Charges Two Canadians with Fraudulently Touting Penny Stocks on a Web Site*, Facebook and Twitter, Press Release No. 2010-114, June 29, 2010, http://www.sec.gov/news/press/2010/2010-114.htm (last visited Apr. 3, 2012).

Apparently, however, the rapper's attorney intervened, and a subsequent tweet by the rapper stated: "I own [company] stock thoughts on it are my opinion. Talk to financial advisor about it."[70]

3. FTC Regulated Entities

In October 2009, the FTC, the federal government's chief guardian against unfair or deceptive business practices, revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising to include social media.[71] The notice incorporated several changes to the FTC's guidelines, which address endorsements by consumers, experts, organizations, and celebrities, as well as the disclosure of important connections between advertisers and endorsers. Specifically, the revised Guides specify that while the FTC will consider conduct and render decisions on a case-by-case basis, the post of a blogger who receives cash or in-kind payment to review a product is considered an endorsement:

> Thus, bloggers who make an endorsement must disclose the material connections they share with the seller of the product or service. Likewise, if a company refers in an advertisement to the findings of a research organization that conducted research sponsored by the company, the advertisement must disclose the connection between the advertiser and the research organization.[72]

In light of these new guidelines, organizations should be aware that the FTC is keeping a close eye on their interactions with bloggers. In April 2010, six months after the revised Guides were released, the FTC made public its first investigation into a company's relationship with bloggers. The case involved a promotion by Ann Taylor, which had invited bloggers to preview the Loft division's summer 2010 collection, offering a "special gift" and promising that those posting coverage from the event would be entered into a "mystery gift-card drawing," where they could win between $50 and $500. The invitation explained that bloggers must submit posts to the company within 24 hours in order to find out the value of their gift card.[73]

The event, coupled with the unusual request for posts to be submitted for a prize, was noticed and analyzed by the FTC.[74] As explained by Mary Engle, the FTC's Associate Director – Advertising Practices, in a letter dated April 20, 2010, to Ann Taylor's legal representation: "We were concerned that bloggers who attended a preview on January 26, 2010 failed to disclose that they received gifts for posting blog content about that event."[75] Although the agency decided not to take action against Ann Taylor, the decision indicates that the FTC is watching these issues closely; and, in addition, it provided some insight into how it is viewing marketers' relationships with online communities.

---

70 Dian Chu, *Hip Hop Social Media Meets Wall Street: 50 Cent and His $8.7 Million Penny Stock Tweets,* EconForecast, January 15, 2011, http://dianchu.blogspot.com/2011/01/hip-hop-social-media-meets-wall-street.html (last visited Apr. 3, 2012).

71 Federal Trade Commission, *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, (effective December 1, 2009), http://www.ftc.gov/os/2009/10/091005endorsementguidesfnnotice.pdf (last visited Apr. 3, 2012).

72 FTC Press Release *FTC Publishes Final Guides Governing Endorsements, Testimonials*, October 5, 2009, http://www.ftc.gov/opa/2009/10/endortest.shtm (last visited Apr. 3, 2012).

73 Natalie Zmuda, *Ann Taylor Investigation Shows FTC Keeping Close Eye on Blogging*, April 28, 2010, http://adage.com/article?article_id=143567 (last visited Apr. 3, 2012).

74 *Id.*

75 Closing Letter to Kenneth A. Plevan, Esq., Counsel for Ann Taylor, April 20, 2010, www.ftc.gov/os/closings/100420anntaylorclosingletter.pdf (last visited Apr. 3, 2012).

The revised Guides prompted questions, and in July of 2010, the FTC published answers to questions regarding the revised Guides.[76] The FTC explained that it revised the Guides to show how they apply to today's marketing world, and it answered several of the most frequently asked questions about the revised Guides.[77]

Because social media can be particularly effective at communicating the efficacy or truthfulness of a regulated entity's sales or marketing claims, the FTC has focused on trying to ensure that consumers are fully informed about who is on the other side of any such communication (e.g., identifying "astroturfing" campaigns by regulated entities). The FTC has also been concerned about payments to Internet users who post positive product reviews on websites and the development of "flogs," which are blogs that appear objective and genuine but are designed to covertly promote a product.[78]

4. Health Care Industries

The importance of regulatory compliance in health care necessitates extra care in the formulation and enforcement of social media policies, as well as consideration of technology tools to support them.

a. Food and Drug Administration

Unlike the FTC, which has been active in providing detailed social media guidance, the U.S. Food and Drug Administration ("FDA") was beginning to develop guidelines regarding social media use to promote FDA regulated products as this Primer was drafted. The FDA held public hearings in November 2009 on "Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools."[79] The FDA's Division of Drug Marketing, Advertising and Communications indicated that the FDA had been researching the following topics in connection with promotion of FDA-regulated medical products on social media: "Responding to unsolicited requests; fulfilling regulatory requirements when using tools associated with space limitations; fulfilling post-marketing submission requirements; online communications for which manufacturers, packers or distributors are accountable; use of links on the Internet; [and] correcting misinformation."[80]

Despite its previous communications, the FDA has still not published comprehensive social media guidelines. In December 2010, the FDA released a document focused on the FDA's "Strategic Priorities: 2011-2015." The document does provide some insight into the future direction of the FDA and offers certain insights regarding its position on social media. It also offers advice that pharma companies considering marketing or communications for a drug, medical device, healthcare organization, or biomedical research organization should heed. But for those awaiting specific guidance on social media usage there is only one point in the entire 48-page document of strategic priorities where social

76 *See* FTC's Revised Endorsement Guides: What People are Asking, http://business.ftc.gov/documents/bus71-ftcs-revised-endorsement-guideswhat-people-are-asking (last visited Apr. 3, 2012).
77 *Id.*
78 Alan Friel, *Navigating FTC's Guidance on Social Media Marketing*, Adweek, Nov. 30, 2009, http://www.adweek.com/aw/content_display/community/columns/other-columns/e3i5bf1e98f0ce98d79ff2629077ea6b78a (last visited Apr. 3, 2012).
79 Transcripts and additional information can be found at http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/UCM184250.htm (last visited Apr. 3, 2012).
80 *Three-Month Pushback Frustrates Industry Digging into Social Media and Internet Advertising*, Advertising Age, December 22, 2010, http://adage.com/article?article_id=147857 (last visited Apr. 3, 2012).

media is even mentioned.[81] On December 30, 2011, the FDA released a limited-scope draft guidance addressing off-label usage of pharmaceuticals.[82] The draft left many questions unanswered.[83]

Industry observers believe that, notwithstanding its lack of guidance on how organizations may utilize social media without violating FDA regulations, the FDA itself intends to actively use social media formats to reach patients, healthcare professionals, and other governmental organizations. Indeed, the FDA has already launched several forward-thinking social media initiatives, including tweeting about FDA Recalls and creating a dedicated YouTube Channel.[84]

b. HIPAA

The use of social media in the health care industry creates unique challenges – perhaps more than in any other industry. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets forth a variety of rules focused on privacy and security of personal health information.[85] Although HIPAA mandates the confidentiality of personal health information, the use of social media by health professionals has resulted in numerous publicized security breaches. For example, seven hospital staff members were fired or disciplined after taking photos of a dying patient and posting them on Facebook.[86] Another hospital fired five hospital employees who "used social media to post their personal discussions concerning hospital patients" on Facebook.[87] Three years ago, the same hospital fired ten staff members for taking photographs of patients and patient records.[88]

A more complex issue is presented by the creation of "health networks" composed of individuals who use social media to share or collaborate regarding health issues.[89] Within these online networks, individuals share personal health information. Users may fail to review carefully the privacy policies of the social media host regarding privacy, use, ownership, or retention of the information. In addition, users may fail to appreciate that other users may violate the privacy terms and share confidential information. There also may be special concerns where the user's posts disclose or suggest personal health information of others. For example, a user might post information regarding a genetic condition that would then suggest familial health information.[90]

---

81 Rohit Bhargava, *The FDA & Social Media: What to Expect in 2011*, December 21, 2010, located at http://www.dailyblogworld.com/post/marketing/the-fda-social-media-what-to-expect-in-2011.aspx (last visited Apr. 5, 2012).

82 U.S. Department of Health and Human Services, Food and Drug Administration, Guidance for Industry Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices, December 30, 2011, http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm285145.pdf (last visited Apr. 3, 2012).

83 See Arundhati Parmar, *FDA's social media marketing draft guidance: a roundup*, MedCity News, Jan. 12, 2012, http://www.medcitynews.com/2012/01/fdas-social-media-marketing-draft-guidance-a-round-up (last visited March 5, 2012).

84 *Supra* n.80.

85 *See Understanding Health Information Privacy,* http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited Apr. 3, 2012).

86 M. Hennessy-Fiske, *When Facebook Goes to the Hospital, Patients May Suffer*, *L.A. Times*, August 8, 2010, http://articles.latimes.com/2010/aug/08/local/la-me-facebook-20100809 (last visited Apr. 4, 2012).

87 *5 Nurses Fired for Facebook Postings*, June 10, 2010, http://www.10news.com/news/23857090/detail.html (last visited Apr. 4, 2012).

88 *Cell Phone Photos led to Hospital Firings*, May 11, 2007, http://www.10news.com/news/13305945/detail.html (last visited Apr. 4, 2012).

89 *See, e.g.*, Patricia Sanchez Abril and Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, Northwestern Journal of Technology and Intellectual Property, Summer 2008, http://www.law.northwestern.edu/journals/njtip/v6/n3/1 (last visited Apr. 4, 2012).

90 For example, California law enforcement arrested a man using familial DNA matching. The son's DNA was taken while in custody and led to a familial match (father) in multiple homicides. A. Fantz, *Accused Serial Killer Snared Using Controversial Technique*, July 11, 2010, http://www.cnn.com/2010/CRIME/07/08/familial.dna/index.html (last visited Apr. 4, 2012).

Such self-disclosure may raise issues regarding eligibility for insurance or insurance benefits. Although insurance companies' advertising regulations may govern their postings to social media sites, another issue is whether insurance companies may use an individual's postings to determine insurability or rates.[91]

An additional complexity arises from social media postings related to mental health. A social media posting might disclose explicitly or implicitly a possible mental health issue, or lack thereof. For example, a Canadian woman on disability leave diagnosed with depression had her insurance benefits cancelled after posting vacation pictures on Facebook.[92] United States courts have ordered production of social media postings of minors related to the causes and symptoms of eating disorders and related to alleged extreme emotional distress in harassment cases.[93]

Social media postings related to mental state may also pose ethical issues for "required reporters" such as schools or medical professionals. For example, many therapists search for patient information posted on social media sites.[94] What are their ethical obligations to report a potential patient threat based on a social media posting?

5. Department of Defense

According to Deputy Secretary of Defense William J. Lynn III, the Department of Defense has recognized "the importance of balancing appropriate security measures while maximizing the capabilities afforded by 21st Century Internet tools," and has issued a policy memorandum on the "responsible and effective use of Internet-based capabilities."[95] The policy seeks to balance DOD's national security mission with the recognized benefits of collaboration, both within DOD and with the general public.[96]

B. Regulatory Compliance Advantages of a Social Media Policy

Regulators have made it clear that regulated entities are likely to benefit from a social media usage policy, and they are encouraging or even requiring regulated entities to maintain one. As the purview of regulators varies, so, too, do their guidelines as to whether entities within their oversight must maintain a policy; and, if so, what it should or must include. Examples range from the FTC (which states that the decision to proceed with an enforcement action will be influenced by the presence or absence of a policy) to FINRA (which requires that regulated entities not only have a policy but that its enforcement be supervised and monitored).[97]

---

91 Susan Stead, *Social Media Meets Insurance Regulation: Where Are We Headed?* June 7, 2010), http://www.property-casualty.com/Issues/2010/June-7-2010/Pages/Social-Media-Meets-Insurance-Regulation-Where-Are-We-Headed.aspx (last visited Apr. 4, 2012).

92 Ki Mae Heussner, *Woman Loses Benefits After Posting Facebook Pics,* Nov. 23, 2009, http://abcnews.go.com/Technology/AheadoftheCurve/woman-loses-insurance-benefits-facebook-pics/story?id=9154741 (last visited Apr. 4, 2012).

93 *See* Mary Pat Gallagher, *Myspace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders*, Feb. 1, 2008 (cases consolidated for discovery: *Beye v. Blue Cross Blue Shield of NJ*, 06-Civ.-5337 (D.N.J. 2008), and *Foley v. Horizon*, 06-Civ.-6219), http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005559933 (last visited Apr. 4, 2012); *EEOC v. Simply Storage Mgmt.*, No. 1:09-cv-1223-WTL-DML (S.D. Ind. May 11, 2010).

94 Dana Scarton, *Google and Facebook Raise New Issues for Therapists and their Clients*, *The Washington Post*, March 30, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/29/AR2010032902942_pf.html (last visited Apr. 4, 2012).

95 DOD Releases Policy for Responsible and Effective Use of Internet-Based Capabilities, U.S. Department of Defense News Release No. 154-10, February 26, 2010, http://www.defense.gov/releases/release.aspx?releaseid=13338, (last visited Apr. 4, 2012).

96 *Id.* The policy, as amended, can be found at http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf (last visited Apr. 4, 2012).

97 16 C.F.R. Part 255 (2009).

PART TWO – E-DISCOVERY ISSUES

Adequate preservation, collection, review, and production of social media content may require specialized attention and cooperation. The purpose of Part II is to provide guidance and a framework for addressing the unique challenges arising from the discovery of social media. The intent is not to supersede *The Sedona Principles* or *The Sedona Commentary on Legal Holds*, but rather to provide additional guidance with respect to those issues unique to social media content.

I. Threshold Issues

A. Relevance

As is the case with other types of electronically stored information ("ESI"), the threshold issue in deciding how to preserve and collect social media content is determining whether the content is relevant.[98] Various courts have already found that social media content that is relevant to litigation is discoverable.[99] For example, one court found that social media might be relevant to understanding the emotion, feeling, or mental state of claimants in a sexual harassment suit.[100] And sanctions are possible for spoliation of social media content, as with any sort of relevant information.[101] Thus, it is clear that social media content that is relevant to reasonably-anticipated litigation must be preserved.[102]

B. Possession, Custody and Control

Another threshold issue is determining whether social media content is in the party's possession, custody, or control such that a party has a legal obligation to identify and preserve it.[103] This determination is complicated for social media content because of the various ways in which the content is generated and stored. An individual user may generate content by uploading it to his or her site. The user, however, may not have access to all potentially relevant social media content and its associated data once the item is posted.[104] The content is typically stored and hosted by a social media service provider and not by the user. If the user-generated content is posted to someone else's social media site, the user may not have any access to the content once it is posted. Additionally, an organization may store social media content generated by users on the organization's internal servers and infrastructure that the users may not be able to access.

98 *Zubulake v. Warburg,* 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*) (party is "under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request").

99 *Bass v. Miss Porter's School*, 2009 WL 3724968 (D.Conn. Oct. 27, 2009) (ordering the production of "more than 750 pages of wall postings, messages, and pictures" from plaintiff's Facebook account); *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (denying plaintiffs' motion for protective order regarding their Facebook, Myspace, and Meetup.Com content); *see also Muniz v. UPS*, 2011 WL 311374 (N.D. Cal. Jan. 28, 2011)(finding plaintiff's counsel's postings on various listservs and social media networks were irrelevant to fee dispute but noting that the type of searching discovery that is typical of issues on the merits is not equivalent to fee litigation).

100 *EEOC v. Simply Storage Mgmt.,* 270 F.R.D. 430 (S.D.Ind. May 11, 2010); *see also Offenback v. Bowman,* 2011 WL 2491371 (M.D. Pa. June 22, 2011).

101 *See Lester v. Allied Concrete Co.,* Nos. CL.08-150, CL09-223 (Va. Cir. Ct. Sept. 1, 2011) (reducing jury award by over $4 million because plaintiff "deliberately delete[d] Facebook photos that were responsive to a pending discovery request" at counsel's direction); *Lester v. Allied Concrete Co.*, Nos. CL08-150, CL09-223 (Va. Cir. Ct. Oct. 21, 2011) (ordering plaintiff and plaintiff's counsel to pay defendants over $700,000 in fees and expenses).

102 "A reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation." *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process*, 11 The Sedona Conference J. 265 at 269 (Fall 2010) *available at* https://thesedonaconference.org/download-pub/470.

103 F.R.C.P. 34(a)(1).

104 There are certain types of data to which the user or subscriber may not have easy access, but to which the service provider does. This can include activity log data showing the date and time the user accessed the site, IP addresses from where the account was accessed, and reports detailing other aspects of the user's social media account.

Whether a user who generated content posted on a social media site has possession, custody, or control of his or her own social media content, thus requiring preservation, is the most straightforward analysis. A user typically has "control" of his or her own social media content – to the extent he or she can still access it – because the user typically has the "legal right, authority, or practical ability to obtain the materials sought on demand."[105] Indeed, some social media sites even specify in their terms of use that users have control of their own content.[106] Thus, a user sued in an individual capacity has a duty to preserve relevant social media content that the individual can obtain on demand.[107]

The determination whether an organization has possession, custody, or control of social media content stored on its internal servers and infrastructure is similarly straightforward. A corporation that has the "ultimate authority to control, to add, to delete, or modify" a website stored on its own servers has possession, custody, or control of the content.[108]

The more difficult analysis is determining whether an organization has possession, custody, or control of relevant social media content posted by an employee on an external social media site, and whether the organization has a duty to identify and preserve social media content stored in this manner. In a similar context, a court held that an individual plaintiff did not have possession, custody, or control of hyperlinks contained in emails wherein the hyperlinks were originally stored on an external remote server but no longer existed and thus the plaintiff did not spoliate evidence by failing to preserve such hyperlinks.[109] This case suggests courts may view social media content posted by an employee on an external site not to be in the possession, custody, or control of the organization, and this view is consistent with the case law relating to an employee's right to privacy. On the other hand, at least one court has ordered a corporation to produce email from personal email accounts from upper-management employees over the corporation's objection that it did not have access to the employees' personal email accounts.[110] Additionally, commentators have suggested that employers that expressly inform their employees that any and all documents and information created, stored, or exchanged from or by the employer's computer and communications systems belong to the employer, or employers that monitor employees' private use of company computers could arguably be held to "control" such information. This may be the case even if the information was created for personal use, and even if physically stored on a third party's servers. The employer thus may have to produce such information if requested in discovery.[111]

C. Ethics

Another issue with the preservation and collection of social media is whether it is even permissible to access social media sites in order to preserve or collect data for use in legal proceedings. Because data posted on social media sites is usually protected by privacy

105 *Steele Software Sys. Corp. v. DataQuick Info. Sys., Inc.*, 237 F.R.D. 561, 564 (D. Md.2006) (citations and internal quotations omitted).

106 "You own all of the content and information you post on Facebook, and you can control how it is shared. ..." Facebook Statement of Rights and Responsibilities, April 26, 2011, Revision, § 2 (http://www.facebook.com/#!/terms.php, last visited on Apr. 4, 2012). In addition, Facebook has a feature allowing users to download content that they have placed on Facebook. *See* Mark Zuckerberg, "Giving You More Control," Oct. 6, 2010, http://blog.facebook.com/blog.php?post=434691727130 (last visited on Apr. 4, 2012).

107 Arteria Property Pty Ltd. v. Universal Funding, 2008 WL 4513696 (D.N.J. Oct. 1, 2008).

108 *Id.*

109 *Phillips v. Netblue, Inc.*, 2007 WL 174459 (N.D.Cal. Jan. 22, 2007).

110 *Helmert v. Butterball,* 2010 WL 2179180 (E.D.Ark. May 27, 2010).

111 *See* Steven Bennett, *Civil Discovery of Social Networking Information*, 39 Southwestern Law Review 413, 419 (2010), http://www.swlaw.edu/pdfs/lr/39_3bennett.pdf (last visited Apr. 4, 2012).

settings and various degrees of permissions, regular Internet searches yield only the limited user profile information that is made publicly available to everyone. When the site provider does not conduct the collection, the process of collecting a deeper cut of social media data typically requires the collector to access the social media site directly. This can be done either by logging on to the site using a personal account or by using software that accesses websites via automated means. Each of these approaches potentially poses ethical issues when data is collected for use in legal proceedings.

As discussed in detail below, there is clear authority against attorney "pretexting"; it is unethical for an attorney to use deceptive means to "friend" or cause another to "friend" a person in order to gain access to postings with heightened privacy settings for use in litigation. Once logged into the social media site, however, a person need not "friend" a second person in order to access his public-facing information. Yet collecting a fellow site user's public-facing information may raise its own issues. While social media sites exist to facilitate the sharing of data, the act of data preservation or collection may violate the social media site's terms of service. Sites may require account holders to adhere to codes of conduct that include refraining from collecting fellow account holders' information without informed consent; it is unclear if this includes collecting data for use in legal proceedings.[112] Penalties for failing to follow a site's terms of service may include termination of the user's account.

In any event, this method of preservation or collection puts the collector squarely in the chain of custody. Using or producing this data during legal proceedings may result in the collector becoming a witness and being required to testify concerning the collection methodology and process.[113] Casual, incomplete collection of social media data may create problems with authentication if the data, collected for a different purpose, is later used to provide evidence of website changes or to support charges of spoliation. For these reasons, thought should be given to using specialized software and the services of competent vendors for social media site data collection.

II. Preservation and Collection Guidance for Social Media

The preservation and collection of social media data poses significant technical challenges and raises evidentiary issues that at this time are only beginning to play out before courts. To the extent that the underlying data is essentially similar to other types of ESI, the same legal standards apply equally to social media data. Social media data preservation and collection practices should accordingly conform to the principles developed for ESI preservation and collection in general.[114] Because, however, social media data is often hosted remotely, is dynamic and collaborative by nature, can include several data types, and is meant to be accessed through unique interfaces, preservation and collection protocols and standards that have evolved for other ESI are often a poor fit.

---

112 *See, e.g.*, "Facebook's Privacy Policy," Sept. 23, 2011, http://www.facebook.com/policy.php (last visited Dec. 18, 2011), addressing the sharing of data posted on Facebook, *and* Facebook "Statement of Rights and Responsibilities," Apr. 26, 2011, http://www.facebook.com/terms.php (last visited Apr. 4, 2012), which states in pertinent part:
"This Statement of Rights and Responsibilities ("Statement") derives from the Facebook Principles, and governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement. ...
5. Protecting Other People's Rights
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.

113 *See, e.g.*, *Toytrackerz LLC v. Koehler*, Civil Action No. 08-2297-GLR, 2009 WL 2591329, at *6 (D.Kan. Aug. 21, 2009) (non-government website printout was inadequately authenticated under FRE 901; to authenticate a website printout, a proponent must present testimony from the person who created the printout to the effect that it "accurately reflects the content of the website and the image of the page on the computer at which the printout was made.").

114 *See, e.g.*, *The Sedona Principles*, Principles 5, 6 and 12, https://thesedonaconference.org/download-pub/81.

What is clear is that failing to collect relevant data from social media sites when a preservation need arises or is anticipated is ill advised because social media sites can terminate an account or membership[115] and delete content.[116] Thus, organizations might consider collecting social media content at the early stages of the e-discovery process for preservation purposes in order to avoid spoliation arguments. For these reasons, preservation and collection strategies are discussed together herein.

The best strategy for handling difficult preservation and collection issues is to confer with opposing counsel and agree on reasonable steps.[117] There will be various circumstances, however, where consultation is not possible, such as when there is no identifiable opposing party or opposing counsel when the duty to preserve is triggered.[118] Thus, organizations need to consider various strategies when consultation with opposing counsel is not possible.

Tools for preservation and collection of social media content are still being developed and are constantly evolving.[119] Because each social media site is unique, the tools used to preserve and collect content from one site may not work for others. Furthermore, although social media sites may be accessed using a web browser, the nature of social media sites makes it difficult to preserve the content as one would with other websites.

Some practitioners resort to capturing and preserving static images as a means of preservation. There is extensive precedent for courts permitting the use and introduction into evidence of static images.[120] Once logged in, the data preserver/collector can access the target user's public-facing social media posts. This access may use technology employed by site users rather than technology employed by the site provider. However, simply printing out social media site data could result in an incomplete and inaccurate data capture that is hard to authenticate, except on the basis of the personal knowledge of a witness.[121] Also, social media sites can contain data and information, such as video content, that cannot be properly collected in the form of static images (i.e., screen shots and .pdf images).

---

115 For example, "Myspace may terminate your Membership at any time, for any or no reason, with or without prior notice or explanation, and without liability." Myspace Terms of Use Agreement, June 25, 2009, ¶ 2 http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Apr. 4, 2012). Similarly, Twitter "reserve[s] the right at all times ... to terminate users or reclaim usernames." Twitter Terms of Service, http://twitter.com/tos (last visited Apr. 4, 2012). And "Foursquare may terminate your access to all or any part of the Service and/or Add-to Link at any time, with or without cause, with or without notice, effective immediately, which may result in the forfeiture and destruction of all information associated with your membership." Foursquare Labs, Inc., Terms of Use, http://foursquare.com/legal/terms (last visited Apr. 4, 2012).

116 For example, "Myspace may reject, refuse to post or delete any Content for any or no reason. ..." Myspace Terms of Use Agreement, June 25, 2009, ¶ 7.1, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Apr. 4, 2012). Similarly, Twitter "reserve[s] the right at all times ... to remove or refuse to distribute any Content on the Services. ..." Twitter Terms of Service, http://twitter.com/tos (last visited Apr. 4, 2012). And Foursquare reserves the right to (i) remove, suspend, edit or modify any Content in its sole discretion, including without limitation any User Submissions at any time, without notice to you and for any reason. ..." Foursquare Labs, Inc., Terms of Use, http://foursquare.com/legal/terms (last visited Apr. 4, 2012).

117 *See The Sedona Conference Cooperation Proclamation* (2008); *In re Facebook PPC Advertising Litig.,* 2011 WL 1324516 (N.D.Cal. Apr. 6, 2011) (ordering parties to meet and confer in order to devise ESI protocols including for Facebook data) *available at* https://thesedonaconference.org/download-pub/173.

118 *See The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* (July 2008) *available at* https://thesedonaconference.org/download-pub/1703.

119 In October of 2010, for example, Facebook added a feature called "Download Your Information," which allows users to download their profile information, contact information, interests, groups, wall posts, and the photographs, videos, and other content posted to the user's profile. See http://www.facebook.com/blog.php?post=434691727130 (last visited Apr. 4, 2011); https://www.facebook.com/help/?faq=18844 (last visited Apr. 4, 2012).

120 *See, e.g.*, *Michigan v. Liceaga*, 2009 WL 186229 (Mich. App. Jan. 27, 2009) (photograph from defendant's Myspace site depicting him holding the gun used to shoot murder victim and "'throwing' a gang sign" was properly used for the purpose of establishing state of mind and intent and also showed his familiarity with weapons); *U.S. v. Ebersole*, 263 Fed.Appx. 251 (3d Cir. Jan. 13, 2008) (Myspace page admitted at revocation hearing provided context for threatening e-mail sent to stalking victim's sister).

121 *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 538, 542-43 (D.Md.2007); Paul W. Grimm *et al.*, *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information,* 42 Akron L. Rev. 357, 368-69 (2009) (discussing standard for authentication of web site print outs); *see also, e.g., Griffin v. State,* 2011 WL 1586683 (Md. Apr. 28, 2011) (trial court's admission of inadequately authenticated Myspace print out was reversible error); *State vs. Eleck*, 2011 WL 3278663 (Conn. App. Aug. 8, 2011) (affirming trial court's exclusion from evidence based on inadequate authentication of a print out of defendant's Facebook account).

Depending on the specific type of information that needs to be preserved or collected, videoing/interactive demonstration software that creates a record of the experience of navigating a site may more accurately represent the dynamic nature of the information, including capturing dynamic and non-text postings such as audio and video materials.

As with all ESI collections, thorough documentation and verification of the process and results is key to ensuring a cogent product that, if challenged, may be supported with affidavits or testimony. Circumstantial evidence may enhance authentication, including the presence of photographs, email addresses, and posting dates.[122] Related data obtained from other sources, including email notifications of posting activity and computer and account usage logs, may provide additional context to aid authentication.

Any collection of social media content can only represent the social media site data at a fixed point in time. And because of the dynamic nature of social media content, the collector may need to perform completely new collections on a periodic basis, should the circumstances demand. Also, any collection will most likely be a visual representation of what may be complex and interactive data captured without the benefit of metadata and logging data, and without the benefit of the useful data that allows the content to be easily navigated and used.

Third-party providers are developing solutions that go beyond capturing static and single point-in-time images from a specific social media site, and instead allow certain content to be downloaded or collected in a way that better preserves the content and captures the unique metadata fields associated with social media data.[123] Properly captured, these metadata fields can assist with establishing the chain of custody, with authentication, and help to facilitate more accurate and efficient data processing and review. Currently, the full range of metadata associated with social media data can only be collected with specialized e-discovery software designed for that purpose.

Social media sites can, and some do, publish rules and specifications that allow application programming interfaces (APIs) to interact with the social media site in order to capture social media site data by automated means.[124] Because these products integrate with the APIs published by the providers, they are better able to filter data and collect social media data in a more defensible manner, including by collecting all available metadata fields for individual social media items and by generating MD5 hash values for collected social media items. The products are multiplying rapidly and undergoing refinement, spurred on by the need to fill the new regulatory niche, with flow-on effects for e-discovery. When properly developed, these products are registered and approved by the provider and their use is subject to specific terms of service for developers.[125]

However, providers may seek to restrict or ban the use of software designed to automate the collection of website data outside of what is permitted by the APIs and the

122 *See, e.g.*, *In re T.T.*, 228 S.W.3d 312, 322-23 (Tex. App.—Houston [14th Dist.] 2007).
123 For example, a "tweet" generated on Twitter or an individual Facebook post contains over 20 specific metadata items. *See* http://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of (last visited Apr. 4, 2012).
124 An API generally is a set of rules and instructions that allow a software program to interact with other software. *See* Wikipedia available at http://en.wikipedia.org/wiki/Api. APIs may not be effective to capture content from all social media sites, and each social media site may operate in a unique way and allow different types of interaction.
125 *See, e.g.,* Facebook "Platform Policies" available at http://developers.facebook.com/policy (last visited Apr. 4, 2012).

terms of service for application developers.[126] Some site providers are working aggressively to prevent such unauthorized third-party access, including seeking criminal prosecutions for violations where the application intentionally circumvents the security protocols and API frameworks of the provider.[127]

III. Preservation and Collection Guidance in Light of the Stored Communications Act

As discussed above, an organization whose duty to preserve has been triggered may lack possession, custody, or control over relevant social media content stored on external websites. Under these circumstances, a litigant may turn to the social media service provider. A major obstacle to obtaining content directly from the service provider, however, is the Stored Communications Act of the Electronic Communications Privacy Act ("ECPA"). The SCA has been interpreted broadly enough to encompass social media content, such as private YouTube videos,[128] wall posts on a restricted-access Facebook account, comments on a restricted-access Myspace account, private messaging on Facebook and Myspace,[129] and restricted electronic bulletin boards.[130] Below is a detailed discussion of the SCA and guidance on how requesting parties can navigate through the statutory framework to attempt to accomplish preservation or collection.

A. Restrictions on Electronic Communication Service Providers

The SCA imposes different levels of restrictions and protections, depending on whether the service provider at issue is providing electronic communication services or remote computing services. An "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications. ... "[131] And, with certain exceptions, the SCA prohibits "a person or entity providing an electronic communication service to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service. ..." [132]

For this restriction to apply, the communication must be in "electronic storage." While this may seem like a common term, for purposes of the SCA, "electronic storage" is limited to the following scenarios:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.[133]

---

126 *See*, *e.g.*, Facebook "Statement of Rights and Responsibilities" available at http://www.facebook.com/terms.php (last visited Apr. 4, 2012):
3. Safety
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.

127 *See*, *e.g.*, *Facebook, Inc. v. Power Ventures, Inc.*, N.D.Cal., No. C5:08-CV-05780-JW, Document 89 (July 20, 2010) (Order denying Facebook's motion for judgment on claim that violating web site terms of service violates California's computer crimes law Cal. Penal Code § 502, but finding that admitted, deliberate circumvention of technical measures taken to block access through third party's site may subject a user to criminal liability).

128 *Viacom International Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264-65 (S.D.N.Y. 2008).

129 *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (C.D.Cal. 2010) (reasoning in part that wall postings on Facebook and comments on Myspace "are in electronic storage" and denying access).

130 *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

131 18 U.S.C. § 2510(15).

132 18 U.S.C. § 2702(a)(1). One obvious exception is that the service provider may disclose the communication to the sender or intended recipient. 18 U.S.C. § 2702(b)(3).

133 18 U.S.C. § 2510(17).

Thus, this section of the SCA only prohibits an electronic communication service from divulging the contents of communications that are either in temporary storage (such as messages waiting to be delivered) or kept for purposes of backup protection.

B. Restrictions on Remote Computing Service Providers

The SCA separately prohibits unauthorized disclosure of communications by those providing "remote computing services" to the public. Under the Act, "'remote computing service' means providing the public computer storage or processing services by means of an electronic communications system. ..."[134] With respect to such service providers, the SCA prohibits the following:

> [A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service –
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. ...[135]

Compared to the restrictions on "electronic communication service providers," the restrictions on remote computing service providers" are broader and are not limited to communications that are in temporary storage or kept for purposes of backup protection.

C. Determining the Type of Service Involved

Whether a service provider is providing an electronic communication service or a remote computing service depends in large part on the specific type of information or data at issue and its current state. The distinction is not trivial, and can sometimes mean the difference between liability and no liability under the SCA.[136] Also, and adding to the complications of this Act, an entity may qualify as providing both types of service, even for a single type of communication.

For private messages, such as email, that have not yet been delivered or read, the service provider typically is considered an electronic communication service provider, and the messages are subject to the SCA because the communication is in temporary intermediate storage pending delivery.[137]

134 18 U.S.C. § 2711(2).
135 18 U.S.C. § 2702(a)(2).
136 *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008) (agreeing that "if Arch Wireless is an [electronic communication service provider], it is liable as a matter of law, and that if it is [a remote computing service provider], it is not liable"), *rev'd on other grounds*, *Ontario v. Quon*, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010).
137 *See Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d at 987 (C.D.Cal. 2010), and cases addressed therein.

For email that has already been delivered and read, however, there is a split of authority. A copy remains on the service provider's server, and a court may decide that the service provider is still an electronic communication service provider and that the communication is still subject to the SCA because it is being kept for backup purposes. For example, the Ninth Circuit has held that:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again – if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user.[138]

However, other courts may disagree. The Federal District Court for the Eastern District of Pennsylvania, for instance, ruled that retrieved email messages, even if still on the ISP's server, are not kept for backup purposes and therefore "retrieval of a message from post-transmission storage is not covered by the Stored Communications Act."[139]

Courts may also conclude that service providers that retain delivered and read email messages are actually remote computing service providers, thus eliminating the "electronic storage" issue altogether. The Federal District Court, Central District of Illinois, so held in a matter involving web-based email:

> Thus, unless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages, and Microsoft is not storing that user's opened messages for backup purposes. Instead, Microsoft is maintaining the messages "solely for the purpose of providing storage or computer processing services to such subscriber or customer."[140]

It is not necessary that a service provider fall into a single category. Whether the service provider is providing an electronic communication service or a remote computing service, or both, can change depending on the state of the message at issue. Thus, for Facebook's and Myspace's private messaging features:

> As respects messages that have not yet been opened, those entities operate as [electronic communication service] providers and the messages are in electronic storage because they fall within the definition of "temporary, intermediate storage" under § 2510(17)(A). As respects messages that have been opened and retained by [the user], ... the ... entities operate as [remote computing service] providers providing storage services under § 2702(a)(2).[141]

These categorizations do not have to be mutually exclusive. The Federal District Court for the Central District of California has held that Facebook wall posts and Myspace comments are not subject to protection as forms of temporary intermediate storage.[142] But the prohibition applicable to electronic communication service providers can still apply

138 *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004).
139 *Fraser v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623, 636 (E.D.Pa. 2001) (holding that retrieval of stored e-mail after retrieval did not violate the SCA).
140 *United States v. Weaver*, 636 F.Supp.2d 769, 772 (C.D.Ill. 2009).
141 *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d at 987 (C.D.Cal. 2010).
142 *Id.* at 988-989.

because Facebook wall posts and Myspace comments are stored for backup as soon as they are made.[143] Additionally, Facebook and Myspace can also be characterized as remote computing service providers with respect to Facebook wall posts and Myspace comments.[144] Thus, Facebook and Myspace are both electronic communication services and remote computing services with respect to wall posts and comments, and the SCA will apply to prohibit the services from divulging the contents of such wall posts and comments.

D. Public vs. Private Issues

The prohibitions in the SCA expressly apply only to those who provide services to the public. They do not apply, for example, to companies that provide email service to their employees.[145]

Additionally, the SCA protections apply only to private communications and not those readily accessible to the general public.[146] For example, if a user's privacy setting for Facebook or Myspace is such that the general public can view Facebook wall posts or Myspace comments, then the SCA will not apply.[147] The SCA will apply, however, to protect Facebook wall posts or Myspace comments if the user's privacy settings limit access.[148] Similarly, the SCA will not apply to an Internet bulletin board where the general public could gain access simply by signing up,[149] but the SCA will apply to Internet bulletin boards that limit access.[150] Similarly, the SCA will apply to protect videos marked as "private" by a user of YouTube.[151]

E. Enforcement of the Prohibition Against Divulging Communications

There are some exceptions that allow service providers to disclose communications.[152] There is no exception, however, under the SCA for civil subpoenas.[153]

143 *Id.*
144 *Id.* at 990.
145 *Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041, 1042-043 (N.D.Ill. 1998).
146 18 U.S.C. § 2511(2)(g).
147 *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d at 991 (C.D.Cal. 2010).
148 *Id.*
149 *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321-22 (11th Cir. 2006) ("In order to be protected by the SCA, an Internet website must be configured in some way so as to limit ready access by the general public.").
150 *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).
151 *Viacom International Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008). YouTube is a remote computing service provider, as it provides video storage services to its users.
152 *See* 18 U.S.C. § 2702(b). One important exception is that governmental entities can compel ECS providers to disclose communications, including those stored with social media sites, pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction for communications that are in electronic storage for less than 180 days. 18 U.S.C. §2703(a). For communications that are in electronic storage for more than 180 days, a governmental entity can require RCS providers to disclose the contents of such communications by obtaining a warrant and showing probable cause just as is required in § 2703(a) and discussed above. 18 U.S.C. § 2703(b)(1). In addition to a warrant, the governmental entity can also compel disclosure of these email communications stored beyond 180 days by obtaining an administrative subpoena under § 2703(b) or a court order under § 2703(d), both of which require a lower reasonableness standard than a probable cause showing under a warrant. *United States v. Ferguson*, 508 F.Supp.2d 7, 9 (D.D.C. 2007). It is important to note that the Sixth Circuit in December 2010 held that the provisions of 18 U.S.C. §§ 2703(b) and (d) that allow for a governmental entity to compel a provider to disclose the contents of email communications stored beyond 180 days without a warrant are a violation of the Fourth Amendment and therefore unconstitutional. *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), *reh'g denied*, No. 08-3997, 2011 U.S. App. LEXIS 5007 (6th Cir. Mar. 7, 2011); *In the Matter of an Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 2010 WL 5437209 (E.D.N.Y. Dec. 23, 2010) (relying on *Warshak*, finding that government can only obtain location of individuals under SCA with warrant based on probable cause due to Fourth Amendment). The Sixth Circuit's rationale is based on its finding that users in most cases have a reasonable expectation of privacy in emails stored with providers such as Google even if the provider reserves the right to access the users' email for certain purposes and thus the Fourth Amendment is implicated when governmental entities compel a provider to surrender the contents of such emails. *Warshak*, 631 F.3d at 274; *United States v. Cioffi and Tannin*, 668 F. Supp. at 390 n.7; Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1029 (April 2010) ("The Fourth Amendment should generally protect the contents of communications stored in 'the cloud' of the Internet, including remotely stored files maintained on a server that is hosted for individual users."); *but see In re United States*, 665 F.Supp.2d at 1224 (stating that users do not have a reasonable expectation of privacy in emails stored with ISPs because the users voluntarily exposed email to ISPs in the ordinary course of business). Thus, in the Sixth Circuit, a governmental entity cannot obtain email communications through an administrative subpoena or a court order under §§ 2703(b) or (d), and is strictly limited to obtaining the communications through a warrant. *Warshak*, 631 F.3d at 274.
153 *Chasten v. Franklin,* 2010 WL 4065606 *2 (N.D. Cal. Oct. 14, 2010); *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d at 975(C. D. Cal. 2010); *Viacom International Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F.Supp.2d 606, 611 (E. D. Va. 2008).

Courts have quashed subpoenas that would violate the SCA if enforced[154] and denied motions to compel that would result in a violation of the SCA.[155] Moreover, courts have held that the users of the services have standing to seek to quash subpoenas directed to third-party service providers when those subpoenas seek the users' electronic communications.[156]

Additionally, the SCA provides for a civil cause of action against service providers that violate the SCA.[157] The aggrieved party may sue for both equitable relief and damages.[158] The minimum that can be awarded is $1,000; and the damages can include actual damages suffered by the plaintiff, any profits made by the violator as a result of the violation, punitive damages for willful or intentional violations, and attorneys' fees and costs.[159]

F. The Prohibition Against Access by Unauthorized Persons

In addition to barring service providers from divulging the contents of communications, the SCA also bars third parties from improperly accessing an electronic communication maintained by an electronic communication service provider. Specifically, with certain exceptions,[160] the Act prescribes criminal penalties and provides a private right of action against anyone who:

> intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. ...[161]

This prohibition can apply to attorneys who, through improper means, gain access to protected content. In 2004, the Ninth Circuit Court of Appeals held that, in light of the SCA and the overbreadth of the subpoenas issued (they had no time or subject-matter limitations), the attorneys who issued subpoenas to the adverse parties' ISP seeking the adverse parties' email;

> "transparently and egregiously" violated the Federal Rules, and ... acted in bad faith and with gross negligence in drafting and deploying [the subpoena]. They are charged with knowledge of its invalidity. ... The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused.[162]

---

154 *See, e.g., Chasten v. Franklin,* 2010 WL 4065606 (N.D. Cal. Oct. 14, 2010); *In re Subpoena Duces Tecum to AOL*, 550 F. Supp.2d 606 (E.D. Va. 2008); *O'Grady v. Superior Court*, 139 Cal.App.4th 1423, 44 Cal.Rptr.3d 72 (2006).

155 *See, e.g, Federal Trade Commission v. Netscape Communications Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000) (denying FTC's motion to compel).

156 *Mancuso v. Florida Metropolitan University, Inc.,* 2011 WL 310726 (S.D.Fla. Jan. 28, 2011) (plaintiff has standing to move to quash subpoenas directed to among other non-parties, Facebook and Myspace, regarding his usage); *Chasten v. Franklin,* 2010 WL 4065606 (N.D.Cal. Oct. 14, 2010) (defendant had standing to move to quash subpoena seeking emails sent from his Yahoo! email account); *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d at 976 (C.D.Cal. 2010) (plaintiff had standing to seek to quash subpoenas directed to Media Temple, Facebook, and Myspace that sought plaintiff's communications); *J.T. Shannon Lumber Co., Inc. v. Gilco Lumber, Inc.*, Case 07-CV-00119 (N.D. Miss, Delta Div, Aug. 14, 2008) (defendants had standing to seek to quash subpoena seeking defendants' e-mail from ISP).

157 18 U.S.C. § 2707. In *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds*, *Ontario v. Quon*, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010), a provider of text messaging services was held to be liable as a matter of law for violating the SCA by releasing transcripts of text messages.

158 18 U.S.C. § 2707(b).

159 18 U.S.C. § 2707(c).

160 18 U.S.C. § 2701(c).

161 18 U.S.C. § 2701(a) (prohibiting improper access); 18 U.S.C. § 2701(b) (criminal penalties); 18 U.S.C. § 2707(a) (private right of action).

162 *Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir. 2004).

The trial court sanctioned the attorneys.[163] Additionally, because the ISP actually responded to the subpoena by providing some email for the attorneys to review, the Court of Appeals held that the victims could maintain civil claims against the attorneys for violating the SCA. The court stated, "The subpoena's falsity transformed the access from a *bona fide* state-sanctioned inspection into private snooping."[164] Thus, the exception under the SCA for conduct authorized by the entity providing the electronic communications service did not protect the attorneys who issued the subpoenas to the ISP.

G. Seeking to Obtain Information Without Violating the SCA

In light of the prohibitions under, and the potential for criminal and civil liability for violating, the SCA, attorneys must take care when seeking discovery of communications protected by the SCA. One obvious way to obtain communications protected by the SCA would be to subpoena or otherwise obtain them directly from the user or subscriber. Doing so would not implicate the SCA.

If it is deemed necessary to obtain protected communications directly from the service provider, then it should be done with the consent of the user or subscriber of the service. The SCA expressly allows a service provider to divulge the contents of a communication if the service provider has the consent of the originator or recipient of the communication.[165] If voluntary consent is not given, then the requesting party may have to seek a court order compelling the user or subscriber to provide the necessary consent.[166]

Obtaining consent, of course, takes time. And while the parties try to negotiate consent, or while the requesting party seeks a court order, information may be lost. For instance, the founder and administrator of one of the Internet's most popular imageboards[167] testified that threads in the site's most popular board "generally speaking" last "from minutes to hours to a few days at maximum."[168]

If there is a risk that evidence may be lost, a requesting party could place the service provider on notice that the requesting party will be seeking consent, whether voluntary or compelled, to obtain the sought-after information. The requesting party can then further request that the service provider preserve or back up the information, and offer to pay the reasonable costs associated with such preservation. Following such notice, the requesting party could contact the service provider and seek assurances that the requested information is being preserved. Sending a preservation letter to a third party, such as a service provider, however, does not necessarily impose a duty upon the third party to comply.[169] Even jurisdictions that recognize a cause of action for negligent spoliation against third parties typically require a contractual duty to preserve, or a special circumstance or relationship between the requesting party and the third party giving rise to a legal duty to preserve.[170]

---

163 *Id.* at 1072.
164 *Id.* at 1073.
165 18 U.S.C. § 2702(b)(3).
166 *See* Defendant Wal-Mart Stores, Inc.'s Motion to Compel Production of Content of Social Networking Sites, Case No. 1:06-CV-01958, 2009 WL 3061763 (D. Colo. May 26, 2009) (granted by minute order dated June 8, 2009, directing that "Plaintiffs shall forthwith execute consents allowing the Social Networking Sites to produce the information sought in defendant's subpoenas.").
167 An imageboard is an Internet bulletin board devoted to the posting of pictures and images.
168 Testimony of Christopher Poole, page 10, lines 18-22, *United States v. Kernell*, Case No. 3:08-CR-142 (E.D.Tenn. April 22, 2010).
169 *See The Sedona Conference® Commentary on Non-Party Production & Rule 45 Subpoenas* (2008), Section II.B.2; *Fletcher v. Dorchester Mut. Ins. Co.*, 773 N.E.2d 420, 424-25 (Mass. 2002) *available at* https://thesedonaconference.org/download-pub/69 (addressing a non-party's duty with respect to preservation).
170 *Mazloum v. District of Columbia Metropolitan Police Dept*, 522 F.Supp.2d 24, 55-56 (D.D.C. 2007).

> Absent some special relationship or duty rising by reason of an agreement, contract, statute, or other special circumstance, the general rule is that there is no duty to preserve possible evidence for another party to aid that other party in some future legal action against a third party.[171]

Some courts recognize that the duty to preserve can arise in relation to a third party when "there has been a specific request to the spoliator to preserve the evidence. ..."[172] A preservation request alone may not, however, be sufficient to trigger a third party's duty to preserve.[173]

If the court has jurisdiction over the third party, another approach would be to seek permission to issue a preservation subpoena to the service provider early in the litigation.[174] At least one court has recognized that "[i]t may be necessary to issue a preservation subpoena to a non-party when the non-party does not have actual notice of the litigation or when the non-party is a corporate entity which typically destroys electronic information by 'performing routine backup procedures.'"[175] A preservation subpoena would not compel the service provider to divulge the contents of any stored communications, but merely preserve them. The only mention in the SCA of preservation by a service provider is in the context of certain government subpoenas.[176]

IV. Review and Production

A. Review

Generally, the way in which social media data will be reviewed for discovery purposes is driven by how that data was preserved and collected and what is feasible under the circumstances. There are several possible approaches to review. One is to review the social media data in the application with which it was collected, such as commercially available APIs focused on marketing and business development purposes. Another is to load the data into an early case assessment or review tool. The choice turns on various factors, including the importance to the case of reviewing the data interactively as it appeared on the social media site and of monitoring how the content changed over time; the volume of the data to be reviewed; whether metadata was collected along with the content; and the ability of the collection application to facilitate coding and to support litigation processing and management needs (including, for example, search, sampling, Bates stamping and other endorsements, redaction, and export).

When the data volume is low or it is important to review the social media data interactively as it was originally displayed on the site or over a certain time period, it may be best to review the social media content using the API used for collection.[177] Available

171 *Koplin v. Rosel Well Perforators*, 241 Kan. 206, 208, 734 P.2d 1177, 1179 (1987).
172 *Oliver v. Stimson Lumber Co.*, 297 Mont. 336, 349, 993 P.2d 11, 20 (1999). The *Oliver* opinion relies on the holding of *Johnson v. United Servs. Auto. Ass'n*, 67 Cal.App.4th 626, Cal.Rptr.2d 234 (1998), which was abrogated in *Lueter v. State of California*, 94 Cal.App.4th 1285, 115 Cal.Rptr.2d 68 (2002).
173 *Andersen v. Mack Trucks, Inc.*, 341 Ill.App.3d 212, 217, 276 Ill.Dec. 203, 210, 793 N.E.2d 962, 969 (Ill. App. Ct. 2003) (finding no special circumstance imposing a duty to preserve evidence when a defendant sent a letter to a third party requesting preservation of the truck's hose that was allegedly the cause of the plaintiff's injury).
174 *Johnson v. U.S. Bank Nat. Ass'n*, Case No. 1:09-CV-492, 2009 WL 4682668 (S. D. Ohio, Dec. 3, 2009) (permitting issuance of a preservation subpoena to third parties prior to Rule 26(f) conference).
175 *In re Nat'l Century Fin*, 347 F.Supp.2d 538, 542 (E. D. Ohio 2004).
176 18 U.S.C. § 2704.
177 When an individual party's own social media content on a third-party site is relevant to litigation, it can undertake the review directly in its account on the third-party site to determine whether it contains potentially relevant and responsive information. *Offenback v. Bowman*, 2011 WL 2491371 n.3 (M.D. Pa. June 22, 2011).

social media marketing and brand-monitoring products can collect an entire site or a single page with its associated content, such as links to other sites and multimedia files, making the review experience similar to the experience the user had when uploading or posting content. This functionality could be important in a trademark or trade dress infringement case; for example, where the way the allegedly infringing mark is displayed throughout a site or sites and over time is critical. Similarly, interactive access may be relevant to understanding the emotional or mental state of claimants in a sexual harassment suit.[178]

Several marketing and branding-tool vendors have added review features such as search and tagging functionality to their products to address e-discovery and compliance issues. However, these tools are still evolving; and before proceeding, litigants should test the review and production features to determine if they will provide efficient review and support litigation production needs.

When large volumes of social media data are involved, it may make more sense to use an early case assessment tool to filter the social media content and a review tool to accomplish the review. Review tools, in particular, are specifically designed to facilitate efficient review, management, and production. Selecting a review tool for social media data may be particularly useful when the case team is most concerned with the text from social media sites as opposed to the way data was displayed on the social media site. Reviewing social media content in a review tool is also practical when the content was preserved and collected in a manner that rendered it more like other types of ESI such as email, enabling reviewers to utilize features such as threading and bulk tagging.

Clustering and near de-duping technology may also be helpful in identifying content from social media data that is similar to and can be grouped with other ESI such as email and loose files. This technology provides fuller context and prevents social media data from being reviewed in isolation. This functionality, which can also allow the review to proceed faster and more efficiently, is optimized when social media metadata is available.[179]

If the social media content is loaded into a review platform, it will be important to consider how the content will be organized as "documents" within the platform. For example, is the document a page, a site, a user's page, an email message, a blog posting, or a photograph? Content may need to be parsed and reconstructed to make it manageable for review as well as to give context.

It is important to remember that most review tools are not currently programmed to mimic the interactive experience of a social media site. The difficulty in collecting metadata associated with the relevant social media content, combined with other issues such as the tendency of social media sites to incorporate content from external sites, can make using a conventional review platform to review social media content inefficient and ineffective.

B. Production

The same analysis that guides the selection of an appropriate review platform also applies to the production of social media data. The issue turns on how important it is to the case for the receiving party to be able to review the social media site data interactively and as it appeared on the social media site. When interactive review is not important, it

178 *EEOC v. Simply Storage Mgmt.,* 270 F.R.D. 430 (S.D.Ind. May 11, 2010).
179 *The Sedona Principles* at 60-66, https://thesedonaconference.org/download-pub/81.

may be sufficient to produce the social media content in a reasonably usable, searchable format with or without metadata. Currently, and especially in cases involving small amounts of social media data, static images or hard-copy print outs are commonly used for review and production.[180]

It will sometimes be important to produce the relevant social media data in an interactive format that imitates the way it appeared on the site. Production in this manner would be consistent with the concept that a reasonably usable production format is typically one that allows the receiving party to make use of data in the same or similar way as the producing party ordinarily maintained the documents.[181]

Some parties are experimenting with producing social media data in a way that enables a requesting party to make similar use of the content within the meaning of Fed. R. Civ. P. 34(b)(2)(E)(ii). One strategy may be to produce static images of the relevant sites so it is clear what the site looked like at a point in time while, at the same time, "friending" the requesting party who can then view the sites interactively; alternatively, the producing party could "friend" the judge who could perform an *in camera* review.[182] Some courts have required parties to provide their social media user names and passwords to their opponents' attorneys so the opposing counsel has direct, read-only access to the accounts.[183] Another strategy may be to give the requesting party access to certain portions of the API used for collection.

Giving the opponent direct access to a database should be a last resort when there is no other way to accomplish production and when it is critical to the litigation that the opponent have interactive and similar use of the content. Several problems arise when a user of a social media site is required to "turn over" the user name and password to the opposing party. First, doing so may violate the social media site's terms of use.[184] Second, many people use the same password for multiple sites.[185] Thus, a litigant turning over a password for a single social media site may, in fact, be handing over the password to other more sensitive websites. Third, at least one social media site has adopted protocols for detecting when users try to access their accounts from a different computer than they normally use, and respond by requiring additional "proof" that the person attempting to login is who they say they are.[186] The additional proof can come in the form of additional security questions, identifying friends in photographs, or entering a birth date.[187] Finally, requiring users to hand over control of their social media accounts presumes that all of the

180 *See, e.g., Bass*, 2009 WL 3724968 (D.Conn. Oct. 27, 2009) (production of relevant pages of Facebook in hard copy).
181 *The Sedona Principles* at 60-66, https://thesedonaconference.org/download-pub/81.
182 *McMillen v. Hummingbird Speedway*, No. 113-2010 CD, 2010 WL 4403285 (Pa. C.P. Jefferson Sept. 9, 2010); *see also Offenback v. Bowman*, 2011 WL 2491371 (M.D.Pa. June 22, 2011) (court obtained plaintiff's log-in information for Facebook and conducted in camera review to determine if the site contained relevant information); *Barnes v. CUS Nashville, LLC*, 2010 WL 2265668 (M.D.Tenn. 2010) (Magistrate Judge offering to set up a Facebook account and to "friend" friends and witnesses of the plaintiff in order to facilitate in camera inspection and expedite discovery).
183 *Largent v. Reed*, No. 2009-1823, 2011 WL 5632688 (Pa. C.P. Franklin Nov. 8, 2011) (ordering plaintiff to "turn over to Defense counsel here Facebook username email and password"); McMillen *v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 WL 4403285 (Pa. C.P. Jefferson Sept. 9, 2010) (ordering plaintiff to provide Facebook and Myspace user names and passwords to defendant's counsel); *but see Piccolo v. Paterson*, No. 2009-04979, (Pa. C.P. Bucks May 6, 2011) (court denied defendants motion to compel access to plaintiff's private Facebook account postings).
184 For instance, Facebook users agree that they "will not share [their] password, . . . let anyone else access [their] account, or do anything else that might jeopardize the security of [their] account." http://www.facebook.com/legal/terms, Section 4 paragraph 8 (last visited Apr. 4, 2012). Facebook's terms of use also prohibit users from soliciting login information or accessing an account belonging to someone else. *Id.* at Section 3 paragraph 5. Similarly, Reddit's terms of use, as last revised on October 21, 2008, state that users "may not authorize others to use [their] Registration Information." http://www.reddit.com/help/useragreement (last visited Apr. 4, 2012).
185 One online survey revealed that 33% of respondents use the same password for every website that they visit that requires a password. http://nakedsecurity.sophos.com/2009/03/10/password-website (last visited Apr. 4, 2012).
186 Facebook, for instance, will block "suspicious logins," which include attempts to login from "an unusual device." http://www.facebook.com/blog.php?post=389991097130 (last visited Apr. 4, 2012). In order to proceed, the user attempting to login must "answer an additional verification question to prove his or her identity as the real account owner." *Id.*
187 *Id.*

content is discoverable. The focus essentially shifts to the forum of the medium as being relevant and away from the content itself. In addition, turning over user name and passwords also provides the opportunity for spoliation as there will be no audit trail of what was deleted or created.

V. Other Challenges to the Discovery and Use of Social Media

Although the usefulness of social media as evidence is readily apparent, there are many potential limitations on the ability to obtain such information in discovery and to use that information in adversarial proceedings. In this section, we discuss whether the use of social media information may be limited by considerations such as privacy and First Amendment issues (such as anonymous posters), unique social media issues in regulated industries, and international discovery and ethical constraints.

A. Challenges of Third Party Discovery

As discussed above, one of the primary issues may be the amount of third-party discovery needed from individual social media users and third party social media sites. In any adversarial proceeding, one should check the social media sites for information regarding their approach to responding to third party subpoenas.[188] Many include information about service of process, what information will be provided, or even fee schedules for searches. In addition, the "terms and conditions" of use for any such site may be important to gain a preliminary understanding of how the specific site has allocated risks and responsibilities regarding content, ownership, and other considerations.[189]

B. Government Use of Social Media and Social Media Collection

Government agencies are increasingly using social media to communicate.[190] As in other social networking contexts, this is a two-way interaction. Individual users can access the agencies' profiles and postings and government agencies also have access to the profiles and postings of individual users. In many litigations, a government agency is a party or it may store information as a third party. As such, a private party may seek to collect and analyze social media data through a Freedom of Information Act request or through a subpoena.[191]

C. Privacy and Anonymity

Social media sites raise a number of privacy-related issues. As with other Web 2.0 technologies, there is a risk of disclosing personal identifying information that can be used to damage the reputation or the financial or physical security of an individual.

188 For more general information regarding an Internet Service Provider's perspective on responding to subpoenas, *see* Electronic Evidence Compliance – A Guide for Internet Service Providers (US Internet Service Provider Association 2003) available at http://publicintelligence.net/electronic-evidence-compliance-a-guide-for-internet-service-providers.

189 *See generally The Sedona Conference Commentary on Non-Third Party Production and Rule 45 Subpoenas*, *available at* https://thesedonaconference.org/download-pub/78.

190 Transparency and Open Government, 74 Fed. Reg 4685 (Jan. 21, 2009) (executive departments ordered to adopt technologies to enhance public participation); *see also* The White House, http://www.whitehouse.gov, urging the public to connect with the White House using a variety of social media sites.

191 For a discussion of government use of social media and attendant risks *see* Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, University of Maryland School of Law No. 2009-41 available at http://ssrn.com/abstract=1493254 (last visited Apr. 4, 2012).

1. User Privacy Settings

Few cases had addressed the distinction between social media communications that the user designates as "private" and those that are publicly accessible until *Crispin v. Christian Audigier*, 2010 WL 2293238 (C.D. Cal. May 26, 2010) and *EEOC v. Simply Storage Mgmt.*, No. 1:09-cv-1223-WTL-DML (S.D. Ind. May 11, 2010), discussed above. The status of communications as "private" or "public" is important in determining whether SCA protection applies as discussed above. Thus, understanding a user's privacy settings may be crucial in conducting discovery.

In disclosing social media in discovery, there is also a consideration of protecting the privacy rights of individuals not parties to the litigation. This issue can arise, for example, when third parties have posted content on a party's social media site, which has then been requested in discovery, and the third party has the expectation that his or her information would be maintained as "private." One court has suggested, based on the user terms of service and privacy policies of popular social media sites that "no person choosing Myspace or Facebook as a communications forum could reasonably expect that his communications would remain confidential, as both sites clearly express the possibility of disclosure."[192] Assuming a court finds that privacy rights are implicated, the question arises about the steps a party must take to protect the third party's privacy rights prior to producing content involving the third party in response to a discovery request. At first blush, it may sound appropriate for the producing party to redact any third-party "private" information that is not relevant to the litigation. This would result in skyrocketing review costs, however, because of the additional review time required to identify the content and make the necessary redactions. The most prudent course of action would be to require the parties to the action to enter into a protective order or confidentiality agreement that protects the confidential nature of the parties' information and also protects the privacy of third-party private information. Additionally, parties may attempt to agree to the production of certain database fields from the social media sites that would intentionally exclude irrelevant "private" third party content.

2. Seeking the Identity of Anonymous Posters

One well-known feature of social media is the ability to post anonymous comments. This practice poses a significant challenge for those seeking to remove defamatory material but who also need to identify the anonymous posters or who seek discovery from them. The Communications Decency Act (CDA) states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. §230(c)(1) (2008). This provision has been used to preclude suits against Internet service providers who have been asked to remove defamatory content. Therefore, a party must proceed in a "John Doe" suit against the anonymous poster and then issue subpoenas that seek information concerning the identity of the anonymous poster.[193]

---

192 *McMillen v. Hummingbird Speedway*, No. 113-2010 CD, Court of Common Pleas, Jefferson County, PA; s*ee also In re United States,* 665 F.Supp.2d 1224 (stating that users do not have a reasonable expectation of privacy in emails stored with ISPs because the users voluntarily exposed email to ISPs in the ordinary course of business); *but see Piccolo v. Paterson*, No. 2009-04979, Court of Common Pleas, Bucks County, May 5, 2011 (refusing to allow defendants' attorneys access to private Facebook postings).

193 Cases and commentators continue to discuss the scope of the CDA. At least one article has questioned whether it should be applied in the context of social media sites that could be characterized as "gossip sites." Skyler McDonald, *Defamation In The Internet Age: Why Roommates.Com Isn't Enough To Change The Rules For Anonymous Gossip Websites*, 62 Fla. L. Rev. 259 (2010).

The process of uncovering an anonymous poster's identity can be difficult as initial subpoenas may simply produce other IP addresses, requiring additional subpoenas regarding that account holder's identity and account ownership. ISPs or social media sites may notify the account holder or poster, and that person may then seek to quash the subpoena. While procedurally this can be done, a separate set of challenges arise because one cannot utilize the Rule 26 meet-and-confer process to talk to "John Doe's" counsel about the appropriate scope of electronic discovery of social media activities in the case.

Federal courts have applied different standards to determine whether an anonymous poster's identity must be disclosed. For example, the Ninth Circuit denied mandamus when the district court ordered disclosure of posters' identities.[194] In its decision in *In re Anonymous Online Speakers*, the Ninth Circuit discusses a variety of different standards employed by courts regarding protection of anonymous online speech. The Ninth Circuit found that the district court erred in applying a heightened standard requiring that the plaintiff be able to prevail on a hypothetical motion for summary judgment before learning the identity of anonymous posters, but there was no clear error in ordering disclosure of the posters' identities.[195] As stated by the Ninth Circuit:

> [W]e suggest that the nature of the speech should be a driving force in choosing a standard by which to balance the rights of anonymous speakers in discovery disputes. For example, in discovery disputes involving the identity of anonymous speakers, the notion that commercial speech should be afforded less protection than political, religious, or literary speech is hardly a novel principle.[196]

Courts may require plaintiffs to meet a higher standard when they are seeking the identities of third-party witnesses. For example, a federal district court applied a heightened standard to efforts to seek the identity of a third-party anonymous poster. In that case, the court found that the plaintiff's argument that the identity of the bloggers might assist his efforts to impeach defendant's testimony was not sufficiently compelling to outweigh the anonymous bloggers' First Amendment rights.[197]

3. Protective Orders and Sealing

There are strong common law and constitutional presumptions in favor of open courts and public access to court files that extend to the filing of pleadings and other court papers, the evidence presented in adjudication, and the bases for the judgment or verdict. Because all federal cases – and increasingly more state cases – are filed and managed electronically, with public access via the Internet, parties may fear the exposure that litigation involving social media may bring, or may use the threat of such exposure to gain unfair advantage in litigation.

In the discovery context – where there is no presumption in favor of public access – parties with significant relevant social media subject to discovery should negotiate an agreement with the other side to keep confidential any sensitive and private social media, and apply for a protective order under Fed. R. Civ. P. 26(c) that restricts the distribution of

194 *In re Anonymous Online Speakers*, No. 09-71265 (9th Cir. July 12, 2010) (discussing differences between political and commercial speech).
195 *Id.*
196 *Id.* (citations omitted).
197 *McVicker v King*, W.D. Pa., No. 09-436, 3/3/10.

the discovery to specified individuals for specified purposes. The standard for such a protective order is "good cause … to protect a party or person from annoyance, embarrassment [or] oppression."[198] If any of the social media discovery is to be filed with the court or used as evidence, the parties should negotiate, and the court approve, a procedure for lodging such discovery with the clerk subject to a determination by the court as to whether sufficient cause exists for filing the material under seal.[199] If the material has already been filed with the court, the standard for sealing the information is necessarily much higher to overcome given the presumption of public access.[200]

D. Ethical Limitations and Social Media

The use of social media by attorneys implicates various ethics rules and canons. This is true both for an attorney's personal use of social media and for understanding how social media generally affects legal practice, including its potential use as evidence.

1. Attorneys' Own Use of Social Media Through Blogging/Commenting

Attorneys should take care to ensure that their use of social media does not violate ethics rules. For example, they should be careful not to unintentionally create an attorney-client relationship through social media and make sure that any use of social media is consistent with ethics rules regarding solicitation or advertising.

Attorneys' or judges' use of social media to discuss cases or those involved in adversarial proceedings may also create an ethics issue. For example, a Florida attorney was disciplined (with a reprimand and fine) for "numerous derogatory remarks about a judge on a public Internet website."[201] An Illinois assistant public defender lost her job and a disciplinary complaint was filed concerning her blog postings that referred to a judge as "Judge Clueless" and which made reference to pending cases, allegedly revealing confidential information and sufficient information to identify participants.[202] Other attorneys have also been reprimanded or disciplined for blog entries regarding courtroom proceedings.[203] Similarly, attorneys and their employers have been sued for defamation based on anonymous online blogging.[204] Judges using social media have also caught attorneys in misrepresentations.[205] Judges, too, have been admonished for Internet postings.[206] Several states have issued ethics opinions regarding judges' use of social media.[207]

198 Fed. R. Civ. P. 26(c)(1)
199 Fed. R. Civ. P. 26(c)(1)(H).
200 *See generally*, *The Sedona Guidelines on Confidentiality and Public Access* (March 2007), https://thesedonaconference.org/download-pub/478.
201 *See Supreme Court Disciplines 33 Attorneys*, Jan. 22, 2009, http://www.floridabar.org/TFB/TFBPublic.nsf/WNewsReleases/31ecd17b99b806a485257546005a210f!OpenDocument (last visited Apr. 4, 2012) *A Legal Battle for Lawyers-Online Attitude vs. Rules of the Bar* NYTimes.com Page 1 of 3. http://www.nytimes.com/2009/09/13/us/13lawyers.html (referring to judge as "Evil, Unfair Witch").
202 *In the Matter of: Kristine Ann Peshek*, No. 6201779, https://www.iardc.org/09CH0089CM.html.
203 California Bar Journal Discipline Summaries, http://members.calbar.ca.gov/search/member_detail.aspx?x=185591 (attorney suspended and fined for not disclosing that he is an attorney during jury selection and blogging about trial while serving as juror); *Judge Reprimands Temp Prosecutor for Personal Blog*, Apr. 28, 2006 (temporary district attorney reprimanded by Court for blog postings re opposing counsel called "juvenile, obnoxious and unprofessional")(last visited Apr. 4, 2012).
204 *See Ward v. Cisco* (defamation case based on anonymous Patent Troll Tracker blog entry later attributed to in-house Cisco attorney Richard Frenkel).
205 *Facebooking Judge Catches Lawyer in Lie*, Sees Ethical Breaches, ABA Journal, July 31, 2009 (attorney requested continuance based on death of father but Facebook postings showed parties and other activities).
206 *In re Complaint of Judicial Misconduct*, No. J.C. No. 03-08-90050 (Judicial Council of the Third Circuit, June 5, 2009); http://www.upi.com/Top_News/US/2010/04/07/Judge-sues-over-alleged-Internet-remarks/UPI-64921270686534 (last visited Apr. 4, 2012).
207 The Supreme Court of Ohio, Board of Commissioners on Grievances and Discipline, Opinion 2010-7 (Dec. 3, 2010) (judges' social media use is permitted and providing guidelines); Florida Supreme Court Judicial Ethics Advisory Committee, Opinion No. 2009-20, Nov. 17, 2009 (judges may not add lawyers who appear before them as "friends" on a social networking site).

2. Attorney Understanding of Social Media as Potential Evidence

Lawyers should be aware of the potential risks to a client from using social media in legal proceedings. Among their duties are those of competence (ABA MR 1.1) and confidentiality (ABA MR 1.6). The disclosure or use of metadata has been discussed in a variety of publications, usually in the context of documents or email. However, metadata concepts can also appear in the context of social networking. For example, geotagging may permit someone to know where a phone was active or a picture taken.[208] Similarly, metadata may be critical to determining the actual author or poster to a social media site.

As part of the duty of confidentiality, attorneys must also consider the possibility that various proceedings will be posted on social media or networking sites. For example, attorneys may need to make clear that videotaped depositions are "attorney's eyes only" and may not be posted on YouTube.[209]

Finally, as in other areas, counsel must be careful regarding the receipt of confidential or privileged information. For example, ABA Formal Op. 05-437 requires a lawyer who received privileged or confidential documents to "promptly notify the sender in order to permit the sender to take protective measures." This may be more difficult in the context of social media where the origin of the information may be unclear. In the context of litigation, counsel may be able to notify opposing counsel and the court. However, in a pre-litigation context, the "sender" whom the attorney should notify pursuant to the rules may not be obvious, or the attorney may receive materials on an unauthorized basis, such as anonymous documents digitally transmitted through a social media site.[210]

The lawyer's difficulties may be compounded if the attorney learns that the client has improperly gained access to an opposing party's social media content or accounts. Several state bar ethics committees have addressed situations where attorneys learn that a client has access to secret materials of an adversary and they have identified a variety of different courses of action, including advising the client that materials cannot be retained or withdrawing from the representation.[211] Courts have disqualified counsel when they received information under suspect circumstances.[212]

3. Attorney Use of Social Media for Formal and Informal Discovery

Attorneys who use social media sites for investigation must remember that the ethical rules and Rules of Professional Conduct do not change simply because social media sources are involved. When investigating witnesses and even potential jurors, an attorney may wish to view the witnesses' or jurors' social media sites.

---

208 *Web Photos That Reveal Secrets, Like Where You Live*, Aug. 11, 2010, http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html (last visited Apr. 5, 2012).

209 *Judge Orders Counsel to Remove Deposition Excerpt From YouTube*, Dec. 9, 2008, http://www.law.com/jsp/article.jsp?id=1202426579607 (last visited Apr. 4, 2012); *Was That a Yes or a No? Depositions in the YouTube Era*, Latham and Watkins, June 2010, http://www.lw.com/Resources.aspx?page=FirmPublicationDetail&searchText=youtube&publication=3547&globalsearchtype=8191 (last visited Apr. 4, 2012).

210 *See* ABA Formal Op. No. 94-382 (07/05/1994) and Model Rule 4.4(b).

211 Phila. Bar Ass'n., Prof'l Guidance Comm., Phila. Ethics Op. 2008-2, 2008 WL 1849685 (Mar. 2008) (attorney who learns client has access to potentially damaging e-mails between opposing party and opposing lawyer must do more than refuse to discuss (husband's access to his ex-wife's email)); Florida Bar Professional Ethics Comm., Op. 07-01 (Sept. 2007) (lawyer whose client improperly obtains opponent's confidential materials must advise client that the materials cannot be retained or used without informing the opposing party).

212 *See, e.g.*, *Castellano v. Winthop*, 27 So.3d 134 (Fla.Dist.Ct.App. 5th Dist. 2010) (firm disqualified after spending more than 100 hours reviewing attorney-client communications and other confidential information from flash drive that client took from opposing party).

A common feature of many social media sites is the ability of users to limit and control access to the content they post.[213] Thus, a lawyer may know that a social media site exists but not be able to access it. While tempting, it may be a violation of the Rules of Professional Conduct for a lawyer to request greater access to a user's account under pretext, without being forthright about the request and fully disclosing the purpose of the request.[214]

Also, the rules limiting discovery apply equally to requests for social media content. While social media provides additional discovery opportunities, misunderstanding social media can lead to discovery abuses. Social media sites have become a substitute for diaries, letter writing, and photo albums. Sending physical copies of photographs to friends and family is becoming obsolete as people share photographs through their social media sites. Similarly, sending several postcards during a vacation may become a thing of the past as users are able to send and post personalized photographs and messages about their vacations through their social media sites using smart phones and other web-enabled devices.

Attorneys should keep in mind the potential breadth of information that can be contained on a social media site. Discovery requests seeking the entirety of a person's social media site without any date or subject-matter restriction can be akin to asking for every photo album that a person has access to, or asking for copies of every letter that the person has ever sent or received. Thus, discovery requests seeking social media content should be narrowly tailored to seek only relevant information. After all, when signing a request for production, attorneys certify that the discovery sought is "not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation," and "neither unreasonable nor unduly burdensome or expensive. ..."[215]

4. Juror's Use of Social Media

The use of social media by jurors can also result in old problems in a new context. Jurors' unauthorized use of social media has jeopardized cases and can result in a mistrial. This includes jurors using social media to comment about pending trials,[216] and jurors using social media sites to investigate the litigants and discover information about the case.[217]

In light of this problem, courts have begun tailoring their jury instructions to specifically address the juror's use of social media sites.[218] In fact, in 2010, the Committee

213 *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp.2d 965 (C.D.Cal. 2010) (addressing limited access to Facebook and Myspace content); *Viacom International Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (addressing limited access to a user's YouTube content).

214 The Philadelphia Bar Association Professional Guidance Committee, in Opinion 2009-2, opined that sending an anonymous friend request to a witness's Myspace and Facebook accounts for the purpose of gaining access to information that is not available to the general public would violate Rules 4.1 and 8.4(c) of the Rules of Professional Conduct. Model Rule 8.4(c) in particular provides that "i[t] is professional misconduct for a lawyer to ... engage in conduct involving dishonesty, fraud, deceit or misrepresentation. ..." *See also* New York City Bar Formal Opinion 2010-2. ("A lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent." However, "an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request.").

215 F.R.C.P. 26(g)(1)(B)(ii) & (iii).

216 *See U.S. v. Fumo*, 2009 WL 1688482, *58-67 (E.D.Pa. 2009) (juror posting vague comments on Facebook, Twitter, and blogs tangentially related to his jury duty not grounds for removal of juror).

217 *See United States v. Bristol-Martir*, 570 F.3d 29 (1st Cir. 2009) (juror's Internet research related to the applicable law grounds for setting aside conviction and remanding for new trial); *People v. Wadle*, 77 P.3d 764 (Colo.App. 2003), *aff'd*, 97 P.3d 932 (Colo. 2004) (juror's Internet research about anti-depressant medication taken by defendant was grounds for vacating conviction and a remanding for new trial); *Wilgus v. F/V Sirius, Inc.*, 665 F. Supp.2d 23 (D. Maine 2009) (juror "friending" plaintiff and viewing plaintiff's Facebook page after verdict and judgment entered was sufficient to require investigation into juror misconduct, but not grounds for new trial).

218 *See, e.g., Martin v. Royce*, 2010 WL 2521063 (N.D.Ind. 2010) (jury instructed not to consult "reference materials ... the internet, websites, blogs" and not to communicate with others about the case on their "cell phone, through e-mail, BlackBerry, iPhone, text messaging, or on Twitter, through any blog").

on Court Administration and Case Management of the Judicial Conference published and circulated to United States District Court judges a suggested jury instruction that specifically instructs jurors that they are prohibited from using these technologies in the courtroom, in deliberations, or outside the courthouse to communicate about or research cases on which they currently serve.[219]

219 The proposed instruction is available at http://www.uscourts.gov/newsroom/2010/DIR10-018.pdf (last visited Apr. 4, 2012).