

# Social & Mobile Media: Discovery Practices & Considerations

Social and mobile media are rapidly converging, and their pairing is an important trend for those concerned with e-discovery. This convergence is driven by the tremendous adoption of the iPhone, the ubiquity of the BlackBerry, and the near-continuous frequency of digital dialogue for work and social reasons.

By Deidre Paknad and Sonia Cheng



Before you get concerned about discovery of social and mobile media, take a close look at how these media provide value to your company. Reach out to your chief marketing officer, look up your company's Twitter and Facebook pages, and explore the role and value social and mobile media play in your company's operations. This understanding can help you be a better business partner and better understand how these media may be relevant to legal matters. Considering discovery requirements without considering business value and role would be shortsighted.

If your company doesn't yet have a strong social media presence, it is likely just a matter of time. Ask your marketing communications counterparts what their aspirations are and you'll be better able to anticipate discovery and plan for efficient processes.

If your company faces a brand or public relations crisis, expect social media to be a pivotal element in response. Companies that use social media to their advantage in these circumstances fare much better than those that don't, particularly because more social media-savvy activists may often be involved in the public relations crises. When members of the litigation team are well educated and prepared, they can better enable effective PR responses, accelerate market recovery and help the company sustain brand value.

The December issue of Harvard Business Review has several important articles on the business and brand importance of social media, including an insightful analysis of the BP Deepwater Horizon disaster and the role social media played in exacerbating the brand crisis. Consider, too, that the speed of social media caught BP off guard in its brand crisis earlier in 2010. When the litigation team enables rather than prevents a speedy response to crises, everyone wins.

## KEY DYNAMICS AND TREND ACCELERATORS

- Accessibility of social media sites and their ease of use on iPhones (and increasingly the very portable iPad.)
- The use of phones as cameras and video cameras and the ease with which social media sites allow people to share these images.
- New social and commercial applications that incorporate a person's ever-changing location (easily captured or indicated from their mobile device) to enhance the experience or consumer offers such as FourSquare, Mizoon, and Facebook Places.
- Location tagging of photos taken from phones or digital cameras (also called geo-tagging) and embedding of the location and other "metadata" into the image or as a readily visible attribute of the image to enhance the information conveyed when the image is shared.

## 8 IMPORTANT CONSIDERATIONS

As companies mature their social media policies to address e-discovery requirements, and as mobile devices open up new types and kinds of information (including new metadata), there are several important considerations. These include the traditional notions of the relevance of the information to the dispute and whether a party has possession, custody and control and, therefore, an obligation to preserve and produce the information. However, social and mobile media also require consideration of regulatory agency requirements (including prohibitions on access) and the ways in which people use social media.

**1. Is there a regulatory requirement to control it?** SEC and FINRA-regulated entities have unique requirements around social media channels that cover company-authored content as well as the individual sites, posts, tweets, and other communications of their regulated employees. FINRA has issued specific guidance

to help companies and employees comply. As with email and other messaging-based communications regulated by these and other dealer/broker governing bodies, the rules and regulations for social media communications are unlikely to be extended to other industries by regulatory agencies. Enlist your compliance and regulatory team to understand what rules apply to your company or industry, especially if you are in the healthcare, pharmaceutical or financial services industries.

**2. Is it relevant?** Relevance of the information sought should continue to be a key guidepost to whether social and mobile media must be preserved or produced. Much like the intense hype around metadata and forensic collection requirements of years past, reason and relevance should prevail.

**3. Is it unique?** For mobile content, consider uniqueness as well as relevance before expensive collection expeditions. Often the same information is available on central email servers, and collection from the device is unlikely to produce any additional unique or relevant information. This is likewise true for internally facing, company-provided social media channel: company administrators often have centralized access to information, and access via employee accounts may not produce additional unique, relevant information.

**4. Is it in your possession, custody and control?** Not all social media are alike. Only a small portion of social media actually falls under a company's possession, custody and control and is therefore information that, if relevant in anticipated or actual litigation, would need to be preserved and perhaps eventually produced. *In Steele Software Sys. Corp v DataQuick Info. Sys. D. Md 2006*, the Court noted that users have control over their own sites and profiles because they have the "legal right, authority, and practical ability to obtain the materials sought on demand." Facebook policy says the account holder "own[s] all of the content and information" posted and "can control how it is shared." ([www.facebook.com/terms.php](http://www.facebook.com/terms.php))

**5. If not in your possession, custody and control, are there prohibitions to your access?** Third-party sites and services used by individuals at their own discretion and for their own accounts may be off limits under the Stored Communications Act (SCA). The SCA limits what the service provider can divulge based on whether it provided storage services or communications services; because the distinction between these two services is less than clear for sites like Facebook and MySpace, the case law is also less than clear. The SCA can and does apply to YouTube videos posted as "private," Facebook and MySpace profile and wall posts when not available to the general public, and similar content communications. Courts have quashed subpoenas that would violate the SCA if enforced, and the SCA bars improper access and provides for criminal penalties (and has sanctioned attorneys for subpoenas granted and acted upon). See *Crispin v Christian Audigier, Inc C.D. Cal May 26, 2010*, *In re Subpoena Duces Tecum to AOL E.D. VA 2008*, *O'Grady v. Superior Court Cal App 2006*, and *Federal Trade Commission v. Netscape Communications N.D. Cal 2000*, among others.

Permission from the account holder may well be required to collect data for litigation; however, courts have been willing to compel such permission. See *Defendant Wal-Mart Stores Inc.'s Motion to Compel Production of Social Networking Sites, Case No. 1:06-CV-01958, 2009 WL 3061763 (May 2009)*.

**6. How do companies collect social media today?** Few companies routinely collect social media for e-discovery purposes today, although there are cases where more than 700 pages of Facebook material were produced. Before conducting any collection, consider the ethics of collecting data that may not be in your possession, custody or control. In addition to SCA prohibitions, pretexting (such as befriending someone to gain access to their profile pages) is unethical. If a person has made information generally available, it may be possible and prudent to collect. However,

**"SCA: COURTS HAVE QUASHED SUBPOENAS AND PENALIZED ATTORNEYS WHEN THEY WERE GRANTED AND ACTED UPON."**

be mindful of the chain of custody this creates and the implications for authenticating the information. While both Facebook and MySpace have terms-of-use policies that restrict collection of user data for some purposes without user consent, it is unclear whether this applies expressly to collection for litigation purposes.

Nonetheless, collecting this information today is a manual exercise because both social and mobile media are not standardized, evolve rapidly and go beyond traditional folder/content and person/account metaphors. Capturing the interactivity is difficult and few third-party services or tools facilitate it today. Facebook and Twitter allow content to be extracted, but its format is not preserved in the extraction process; nonetheless a chronological “transcript” may be suitable for early case assessment and to facilitate review even though alternative forms of collection may be needed for production.

Collecting social media from third-party services is done page by page, often by creating an image of the page or capturing the page in PDF; this is tedious work because it requires the collector to pay special attention to the comments, threads, “likes” and links on any given page and to ensure these are woven together in a proper replica (which may be a subjective assessment). An alternative to page-by-page collection are tools used to capture software demonstrations. Such tools capture pages, click sequences, links, interactivity, and navigation. Corporate training departments may already have these tools and skills to operate them available in-house, but advice of counsel or experts is important because the law is unsettled in this area.

We anticipate that social media – whether controlled by the company or not – will increasingly be a source of information for employment-related disputes. A careful review of open disputes may be warranted to determine if a change in hold or collection scope is appropriate; the demographics of the workforce may weigh into the decision, but

note that the fastest growing segment of social media users is women over 35 years old.

**7. How much will this cost?** There are several ways to control costs and reduce surprises on social and mobile media discovery. The first and perhaps best practice is to ensure that in-house and outside counsel understand the company’s current technologies and capabilities and current limitations; this ensures that preservation and production agreements are entered into with eyes wide open. Use the Sedona Cooperation Proclamation to control the scope and expense of discovery at the earliest stages of the matter. Attention to the first six considerations in this article can contain costs as well.

**8. Can social media level the playing field in traditionally lopsided discovery situations?** While many companies are focused on the challenges social media presents in e-discovery, it may well be a boon to corporate litigants – one that re-balances discoverable information for individual plaintiffs and corporate litigants. Where historically corporations had vast amounts of information subject to preservation or production requirements, individual litigants generally produced very little data. Behaviors associated with social and mobile media tend to be free-wheeling and over-communicative, and conversation and content more prolific. Corporate litigants should consider the utility of social media, particularly semi-public information and that which an individual plaintiff should preserve and potentially produce. Moreover, location and status information over time, patterns of behavior, state of mind or emotions, and other insights are unique to the social media phenomenon.

## INFORMAL SURVEY OF CGOC MEMBERS – PREVAILING PRACTICES

Practices for preserving and collecting information from mobile devices appear to be concentrated around company-issued devices and typically rely on centralized email servers.

	EXAMPLES OF COMPANY-MANAGED MEDIA	ATTRIBUTES	EXAMPLES OF MEDIA MANAGED BY INDIVIDUALS	ATTRIBUTES
<b>SOCIAL</b>	<p>Company Facebook page, comments, photos, and applications hosted by Facebook or a similar third-party entity.</p> <p>Interactive, collaborative company directory (Ning, Socialcast, Drupal, or other technology) hosted in the company data center or at a third-party under a company account.</p> <p>Company electronic bulletin boards for customers and/or employees hosted by the company or a third-party service provider on the company's behalf.</p>	<p>Branded effort intended to promote products or company brand.</p> <p>Company authorized use; policies can effectively control what is published (either through prior review or policing and removing non-compliant materials).</p> <p>The company has possession, custody and control in fact and in operation. Employee access is via company-created or managed service.</p> <p>Password and access controls are centrally administered by the company.</p>	<p>Individual Facebook, MySpace, LinkedIn and other social or professional profiles.</p> <p>Picasa, Smilebox, YouTube, and other photo and video sharing sites.</p>	<p>Account is opened by an individual acting on their own behalf.</p> <p>Passwords and privacy settings are managed by the individual.</p> <p>Individuals are able to prevent company access or decline to provide passwords to their personal accounts.</p> <p>Individual is able to publish, post, tweet, or convey without pre-screening, and employer has little recourse to demand removal/withdrawal.</p>
<b>MOBILE</b>	<p>Company-provided cell phone or PDA with capability to email, manage calendar appointments, take photos and videos, and text messages.</p> <p>Device may have more capabilities than covered in company policy or controlled through prohibition or monitoring.</p>	<p>Messaging passes through company infrastructure, including mail and messaging servers</p> <p>For business continuity reasons or regulatory requirements, email is stored on centralized company servers (even when an additional copy may be stored on the employee's device)</p>	<p>Employee-purchased cell phone or PDA based on personal preference rather than company business – typically iPhone or iPad.</p> <p>Typically includes many applications that are interactive, and generate information on the individual's whereabouts, likes and dislikes, communications and associations.</p>	<p>Like personal computers and laptops at home on which employees may from time to time do company business.</p> <p>Account is generally held in the employee's name; company policy may state that the device is not formally supported or not allowed.</p> <p>Individual is able to download any variety of application and delete information at will.</p>

- Companies preserved email (often by saving all emails) on the Blackberry Enterprise Server or Domino Server. Mobile access to email is viewed as just that – access – rather than the central storage location or single instance of messages and calendar information.
- As a result, companies tended to target that server location for email collection and bypass the device itself as a collection target.
- For financial institutions, text messaging from mobile devices was carefully controlled and monitored for regulated personnel, and instant messaging was centralized (and therefore managed at the server).
- Across the financial services, automotive, healthcare, and pharmaceuticals industries, companies noted infrequent collection of text, images and data saved locally on a device (that is not also saved on a central server). Government inquiry, employee disputes and internal investigation were cited as the types of matters in which manual collection from a device may be required.
- A number of companies reported standard custodian interview questions regarding mobile device use and habits.
- Some companies – in particular those with strong intellectual property protection practices – were exploring new Blackberry

Enterprise Server (BES) generations that allow remote deletion of device data in the event of loss or theft. IP concerns also led some companies to prevent storage on the device since previous generations of BES did not enable remote deletion.

- Most seem to rely on company-issued devices as the source of potentially relevant information and to rely on company policy regarding their use as a “boundary” for discovery practices.
- With email as frequent a target of litigation as it is for these companies, their practices were reasonably routine and may have been the subject of test or significant inquiry by other parties.

On the other hand, practices for preserving and collecting social media were less defined. A number of companies had no e-discovery experience yet in this area. Current practices included:

- Most companies operate Facebook pages, Twitter accounts and other public-facing social media to promote products and foster consumer, customer or market goodwill. Like other public-facing promotional efforts, these sites and accounts are centrally managed and monitored, typically by marketing communications and public relations personnel.
- Most also provided internal social media applications for internal employee use. The internal applications functioned similarly to earlier generation bulletin boards and collaboration sites. These internal sites

enable discovery from central servers in much the same way email archives and BES enable access to custodian data.

- Companies are now exploring the implications and obligations for preserving and collecting data from their internally-facing and externally-facing sites.
- Some have begun to explore and define what obligations may extend to third-party hosted sites and content not authored by authorized company staff as well as how posted content in these sites may be of utility in their own claims or defenses.
- No company cited the need for or had identified an enterprise-grade social or mobile media collection automation tool.

## RECOMMENDATIONS

If you're not familiar with the spectrum of social and mobile media shown in the previous chart, get educated. Here are five simple ways to develop understanding and intuition that can help you reduce risk and increase your advantage in litigation:

1. Ask a teenager or a middle-aged woman how they use Facebook and other social media and listen intently!
2. Set up your own LinkedIn and Facebook profiles and use them consistently for a month.
3. Ask your marketing communications manager what their “social media strategy” is and why; ask to see what the prevailing social media behaviors are across the company’s target customers (which likely inform the social media strategy and are equally informative to your discovery efforts).
4. Buy an iPhone or iPad and explore. Use it to communicate with family who text and exchange photos and videos frequently.
5. Shift from dread and denial to adoption and acceptance; the legal department cannot turn back the tide, but it can ride the wave.



## CASES OF NOTE

- *Bass v. Miss Porter's School (D. Conn 2009)* – relevance and discoverability of social media and ordering production of more than 750 profile pages
- *EEOC v. Simply Storage Management LCC (SD Ind May 2010)* – defendant sought and won discovery of plaintiff's MySpace and Facebook pages to assess plaintiff's claims of emotional distress
- *Crispin v Christian Audigier, Inc C.D. Cal May 26, 2010* – interpretation of SCA scope to wall postings
- *Ledbetter v. Wal-Mart Stores (D. Colo 2009)* – granting discovery of plaintiff's Facebook, MySpace and other social media content
- *Defendant Wal-Mart Stores Inc.'s Motion to Compel Production of Social Networking Sites, Case No. 1:06-CV-01958, 2009 WL 3061763 (May 2009)*— ordered plaintiff to execute consent for service providers to produce information sought by defendant

## ABOUT THE AUTHORS

### Deidre Paknad

CGOC Founder and Director of Information Lifecycle Governance Solutions at IBM. Deidre is widely credited with having launched the first commercial applications for legal holds, collections and retention management and is a recognized thought leader in legal and information governance with numerous patents in the field. In 2004, she founded the CGOC and has authored many papers in the eDiscovery and governance field. She has been a member of several Sedona working groups since 2005 and co-leads the EDRM IGRM Initiative. Deidre is a seasoned entrepreneur and executive with 25 years' experience applying technology to inefficient business processes to reduce cost and risk. Deidre was inducted into the Smithsonian Institution for innovation in 1999 and again in 2000. Today, she leads IBM's Information Lifecycle Governance business which include

its eDiscovery, records and retention, archiving and defensible disposal solutions. A prolific social media user, she is on Twitter @ day\_dree.

### Sonia Cheng

Director of Client Services, PSS Systems, an IBM Company. Sonia manages the Solutions Consulting practice and is responsible for client delivery success at PSS Systems. She has led legal hold and retention management implementations since 2005, helping companies such as Novartis, JP Morgan Chase, Volkswagen, Kaiser and many others. Sonia has deep experience in enterprise software and holds an engineering degree in Operations Research from Cornell University. An active social and mobile media maven, she is on Twitter @ soniacheng.

## ABOUT CGOC

The CGOC (Compliance, Governance and Oversight Council) is a community of experts in information governance. Its charter is to create a forum in which legal and compliance executives can get the insight, interaction, and information they need to make good business decisions. Established in 2004, it fills the critical practitioners' gap between EDRM and The Sedona Conference. CGOC provides corporate litigation, discovery, IT, and records management leaders and practitioners with educational seminars, benchmarking surveys, group workshops, an annual summit and retreat, white papers by expert faculty, regional working groups, and a social media site for professional networking at [pn.cgoc.com](http://pn.cgoc.com).