MAYER · BROWN

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

March 10 & 11, 2014

The Ritz-Carlton Chicago
160 East Pearson Street
Chicago, Illinois

MAYER·BROWN

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Table of Contents

Agenda

MAYER·BROWN

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Agenda

March 10th & 11th, 2014

The Ritz-Carlton – Chicago, Illinois

Monday, March 10th, 2014

1:00 pm – 1:30 pm: ***Registration***

1:30 pm – 3:00 pm: **Workshop 1: Social Media Content and the Role it Plays in E-Discovery**

Sponsored by iDS

- The phenomenon of social media – and how activity is generating actionable data
- How to identify, collect and analyze data
- E-Discovery challenges for internal social media sites
- What is considered "normal course of business" by a corporate employee?
- Litigation, regulatory and compliance considerations

Speakers: *Daniel Regard, CEO, iDS*
Anthony Diana, Partner, Mayer Brown LLP

3:00 pm – 3:15 pm: ***Break***

3:15 pm – 4:45 pm: **Workshop 2: Social Media Boot Camp**

Social Media: 101. A primer course covering the topics of employment, intellectual property, privacy and litigation, in preparation for more comprehensive discussions on the second day of the Conference.

Speakers: *Richard Assmus, Partner, Mayer Brown LLP*
Matthew Marmolejo, Partner, Mayer Brown LLP
Jeffrey Taft, Partner, Mayer Brown LLP
Lori Zahalka, Associate, Mayer Brown LLP

4:45 pm – 5:30 pm: ***Welcome Reception***

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Tuesday, March 11th, 2014

7:30 am – 8:30 am: ***Registration and Breakfast***

8:30 am: ***Welcome Remarks***

8:40 am – 9:00 am: **Keynote Presentation: Where the Landmines are Buried**

Gain insight from one of the leading cyberspace and First Amendment law scholars in the US, who has been blogging since 2002 and is now blogging at the *Washington Post.*

Speaker: *Eugene Volokh, Professor of Law at UCLA School of Law*

9:00 am – 10:00 am: **Social Media in the Workplace: The Latest Challenges**

- Discharging or disciplining employees for social media activity
- Employer handbook policies restricting employees' social media use
- Employer surveillance of employees' social media activity

Speakers: *Marcia Goodman, Partner, Mayer Brown LLP*
Charles Broll, General Counsel, Nestlé Waters
Katherine Wren, Corporate Counsel, Caterpillar Inc.
Sandra Zubik, Senior Counsel – Labor & Employment and Litigation, Hillshire Brands

10:00 am – 10:15 am: ***Break***

10:15 am – 11:00 am: **Crisis Mode: What Can Be Done? What Should Be Done?**

- Legal options in response to a crisis
- Case studies – the good, the bad and the ugly
- Practical evaluation of alternatives

Speakers: *Carmine Zarlenga, Partner, Mayer Brown LLP*
Cari Brunelle, Partner, Hellerman Baretz Communications
Randy Boyce, Senior VP & General Counsel, Foster Farms
Lee Soffer, Attorney, Nestlé Waters

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

11:00 am – 11:45 am: **Social Media for Corporate Lawyers**

- Implications of Federal securities laws on the use of social media by public companies in communicating with the public
- Use of social media in disseminating corporate information and requirements of Federal securities laws
- Potential liability that may arise when companies, their employees and others share information via social media
- Social media and M&A – due diligence and communications issues

Speakers: *Eddie Best, Partner, Mayer Brown LLP*
Daniel Horwood, Associate General Counsel, Corporate & Securities and Assistant Secretary, Groupon
Christine Ieuter, Director of Corporate Finance, Allstate

11:45 am – 1:00 pm: ***Lunch***

1:00 pm – 1:45 pm: **The Disruptive Business Practices of Social Media – and its Litigation Risks**

- What legal and business issues do companies need to focus on when developing and implementing consumer-facing social media programs
- How to reduce litigation risks
- Update on current litigation trends

Speakers: *John Nadolenco, Partner, Mayer Brown LLP*
Laura Corridon, Counsel, Follett Corporation
Angela Saverice-Rohan, General Counsel & Chief Privacy Officer, Spokeo

1:45 pm – 2:45 pm: **Anticipating the Risks of Government Enforcement and Private Litigation in Social Media**

- What types of social media activity will lead to attention from government officials?
- What are the risks of private class action litigation including privacy class actions?
- What steps should businesses take when facing a government investigation or lawsuit arising from social media?

Speakers: *Marcus Christian, Partner, Mayer Brown LLP*
Archis Parasharami, Partner, Mayer Brown LLP
Jack Halprin, Head of eDiscovery, Enterprise, Google

2:45 pm – 3:00 pm: ***Break***

3:00 pm – 3:45 pm: **In-House Responses to Social Media IP Issues: Benchmarking, Best Practices and Recent Cases**

- Comparing how corporate legal departments manage IP risk in social media
- Best practices for mitigating the IP risks
- Recent cases at the intersection of social media and IP law

Speakers: *Richard Assmus, Partner, Mayer Brown LLP*
Matthew Griffin, Senior Counsel – Enhancers & Trademark, Kraft Foods Group
Jason White, Attorney, General Motors

3:45 pm – 4:45 pm **Social Media: Can it have a Role in Internal Investigations without Ethical Sanctions against Company Counsel?**

- Courts' expansion of the privacy protections for individuals' social media communications
- How companies are faced with the reality that social media is being used to discuss relevant business communications
- Whether companies' legitimate business needs to determine if social media communications are relevant to key issues, such as ongoing litigation and internal investigations, are in line with privacy restrictions

Speakers: *Bill Michael, Partner, Mayer Brown LLP*
Michael Lackey, Partner, Mayer Brown LLP

4:45 pm – 5:00 pm: **Closing Remarks**

MAYER·BROWN

The Social Media Evolution

Social Media Content and the Role It Plays in E-Discovery

Daniel Regard
CEO
iDS
202-249-7877
dregard@idiscoverysolutions.com

Anthony Diana
Partner
Mayer Brown LLP
212-506-2542
adiana@mayerbrown.com

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Daniel Regard
iDS
dregard@idiscoverysolutions.com

Anthony Diana
Mayer Brown LLP
adiana@mayerbrown.com

MAYER·BROWN

The Social Media Evolution

Social Media Boot Camp

Richard Assmus
Partner
Mayer Brown LLP
312-701-8623
rassmus@mayerbrown.com

Matthew Marmolejo
Partner
Mayer Brown LLP
213-621-9483
mmarmolejo@mayerbrown.com

Jeffrey Taft
Partner
Mayer Brown LLP
202-263-3293
jtaft@mayerbrown.com

Lori Zahalka
Partner
Mayer Brown LLP
312-701-7921
lzahalka@mayerbrown.com

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Rich Assmus
Mayer Brown LLP
rassmus@mayerbrown.com

Matthew Marmolejo
Mayer Brown LLP
mmarmolejo@mayerbrown.com

Jeffrey Taft
Mayer Brown LLP
jtaft@mayerbrown.com

Lori Zahalka
Mayer Brown LLP
lzahalka@mayerbrown.com

Social Media Evolution

MAYER·BROWN

Employment

Social Media & Employment Law

- Using Social Media to Screen Applicants
- Issues that Arise During Employment
  - Social Media Policies
  - Monitoring Employee Social Media Activity
  - Bring Your Own Device
- Restrictive Covenants: Non-Solicitation & Non-Competition Agreements

Using Social Media to Screen Employees

- Social media sites may provide information that a company cannot consider in hiring decisions.
- Knowing such information puts a company at risk of claims.
  - Protected characteristics (federal or state law)
  - Prior claims
  - Credit history
  - Criminal history
  - Union activity/complaints about employment conditions

Social Media Policies

- Provide specific guidance on what is and what is not permissible.
- Inform employees that company may monitor all uses of workplace computers, including social media use (and if necessary, inform employees that off-duty use also may be monitored - e.g., securities industry).
- Expressly incorporate other key policies (*e.g.*, discrimination, harassment, confidentiality, technology, codes of conduct).
- Make clear who can and cannot speak on the company's behalf.
- Discuss ownership of company-owned accounts.
  - Including authorized users, treatment of login information, post-termination issues

NLRB Perspective: Social Media Policies

- NLRB General Counsel's office issues 3 Social Media Reports.
  - First Report: August 18, 2011
  - Second Report: January 24, 2012
  - Third Report: May 30, 2012
- Take-home messages from reports:
  - Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.
  - An employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.

NLRB Perspective: Social Media Policies

- A social media policy will violate the NLRA if it "would reasonably tend to chill employees in the exercise of their Section 7 rights."
- A social media policy that does not contain an explicit restriction will still violate the NLRA if:
  - Employees would reasonably construe the policy to prohibit Section 7 activity;
  - The policy was created in response to protected activity; or
  - The policy was applied to restrict an employee's Section 7 rights.

Adopting a Social Media Policy: Example

Original Policy (GC Memo – Unlawfully Broad)

Policy prohibited discriminatory, defamatory, or harassing Internet posts about specific employees, the work environment, or work-related issues on social media sites.

Modified Policy (GC Memo – Lawful)

Prohibited the use of social media to post about coworkers, supervisors, or the Employer that are vulgar, obscene, threatening, intimidating, harassing, **or a violation of the Employer's workplace policies against discrimination, harassment, or hostility, on account of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, statute, or characteristic.**

Reasoning: The second policy would not reasonably be construed to apply to Section 7 activity because it appears in the context of a list of plainly egregious conduct.

Monitoring Employee Social Media Activity

- Practical Considerations:
  - Ensure activity is not interfering with work
  - Ensure employees are following company policies
  - Helps prevent false advertising claims
  - May be required by law in some industries
- Legal Considerations:
  - National Labor Relations Act
  - Stored Communications Act
  - State laws on off-duty conduct
  - State statutes addressing electronic monitoring
  - Common law right to privacy

Bring Your Own Device ("BYOD")

- Why Permit Use of BYOD Devices?
  - Companies need not invest in devices.
  - Employees can choose device.
  - Employees can more easily work remotely or outside regular hours.
  - Some employees are already using personal devices informally for work purposes anyway, without the employer's knowledge or permission.

Bring Your Own Device ("BYOD")

BYOD Concerns

- IT
  - Hardware/software compatibility
  - Tech support for multiple platforms/devices
- Legal
  - Loss of confidential information
    - Unsecured networks provide entry points for hackers.
    - Mobile devices are easily lost or stolen, resulting in loss of confidential information.
    - Employee retention of information post-employment not secure or desired.
  - Access to information for litigation/investigations
  - Protecting privacy of customer/employee data (HIPAA, GLBA)

Post-Employment Actions

Restrictive Covenants/Non-Solicitation/Non-Competition

- Confidentiality or non-disclosure agreements are commonly used to require employees to protect trade secrets and other confidential information of the employer.
- Courts starting to recognize social media-based information as confidential or trade secrets.
  - *NDSL, Inc. v. Patnoude*, 2012 WL 6096584 (W.D. Mich. Dec. 7, 2012) – Former employee contacts employee of former employer's partner via LinkedIn. Injunction denied because not a solicitation.
  - *Christou v. Beatport*, 2012 WL 872574 (D. Colo. Mar. 14, 2012) – Nightclub's patron contact list could be a trade secret.
- Cover specifically in agreements.
- Send **reminder letters** that employer expects compliance with applicable restrictive covenants and confidentiality agreements.

Intellectual Property

Intellectual Property Agenda

I. Managing Your IP Rights on Social Media Platforms

II. Protecting Against Third-Party Infringement Claims

III. Monitoring and Addressing Third-Party Use of Your IP on Social Media Platforms

IV. Striking the Right Balance Between Engaging Your Audience and Protecting Your IP

Managing Your IP Rights on Social Media Platforms

- Before you upload content to any social media platform, there are a few key questions to ask about ownership and control of your IP on that platform:
  - Do you retain ownership of content?
  - What rights are you granting and to whom are you granting them?
  - What happens when you delete your content?
  - What steps should you take to make sure *your* use of your IP does not diminish your rights in trademarks and trade secrets?
- To answer these questions, make sure to review the Terms of Service of each platform you use.

Managing Your IP Rights on Social Media Platforms

- Do you retain ownership of content?
  - Typically, you retain ownership of any content contributed to a social media platform:
    - For example: Twitter - "You retain your rights to any Content you submit, post or display on or through the Services."

Managing Your IP Rights on Social Media Platforms

- What rights are you granting and to whom?
  - Uploading content typically requires you to grant very broad licenses.
    - Usually non-exclusive, worldwide, royalty-free, and transferable
  - Such licenses often allow the social media platform, other users, and sometimes third parties to:
    - Use, transmit, reproduce, publish, publicly perform, publicly display, distribute your content, and to modify, adapt, delete from, add to, and prepare derivative works
  - Often, platforms and other users are not limited to using your content on the original platform where the content was posted.

Managing Your IP Rights on Social Media Platforms

- Example of Licenses You Grant to Social Media Platforms:
  - **foursquare**:
    - License Rights: Any use, at foursquare's sole discretion
    - License Granted To: foursquare and its users (including third-party media organizations)
    - License Scope: No limitations; your content can be used for any purpose

Managing Your IP Rights on Social Media Platforms

- What happens when you delete your content?
  - Don't assume that deleting content automatically terminates any licenses you granted.
  - To the contrary, social media platforms typically have terms that dictate:
    - How quickly the platform will remove your content upon request
    - Whether the license terminates when you delete your content
    - What the platform (and its users) can do with deleted content

Managing Your IP Rights on Social Media Platforms

- What steps should you take to make sure *your* use of your IP does not diminish your rights in trademarks and trade secrets?
  - Implement and regularly update a comprehensive social media policy or plan to provide guidance to your employees about the risks inherent in using social media
  - A social media plan should at least address the following:
    - What content can and cannot be uploaded to social media platforms
    - Who may and may not post content on behalf of the organization
    - How uploaded content should be monitored
    - Policies and procedures for removing content and monitoring content removal by the platform

Protecting Against Third Party Infringement Claims

- Always consider how your use of social media implicates *third- party* intellectual property rights.
- Two areas to keep in mind:
  - Rights Clearance
  - Dealing with User-Generated Content

Rights Clearance

- Review social media campaigns and your company's use of social media for potential issues involving:
  - Licenses – confirm that licenses to third-party content grant the ability to use that content on social media
  - Trademark infringement – confirm references to marks you do not own are permitted
  - Copyright infringement – ensure that your use of images, written work, video, music, etc. is permissible
  - Rights of publicity – confirm you have authorization to use images or likenesses of recognizable people (including non-celebrities)

Rights Clearance

- Tips:
  - Treat social media as you would your other advertising platforms and ensure all content has been fully cleared for potential IP issues (and remind employees to do the same!)
  - Obtain licenses before using content generated by other users

User-Generated Content

- Remember that, by soliciting and displaying user-generated content, you may open yourself up to liability for hosting infringing content
  - Safe Harbor Protection under DMCA 512(c) requires:
    - No actual knowledge of infringement
    - No direct financial benefit
    - Expeditious takedown after qualifying notice
    - Designation of a DMCA agent
    - Implementation of reasonable repeat infringer policies
    - No interference with standard technical measures

Monitoring and Addressing Third-Party Use of Your IP

- To protect your brand and your content online, be on the lookout for:
  - Copyright Infringement
  - Trademark Infringement
    - On social media platforms, this may take a variety of forms
      - True "fan" accounts, pages, handles – fans that are celebrating your brand, but using your IP to do so
      - Parody accounts, pages, handles – users often pose as a famous character or brand for comedic purposes
      - Brand-jacking/username squatting – third parties that use your brand in handles, vanity URLs, etc. without authorization

Monitoring and Addressing Third-Party Use of Your IP

- Enforcing your rights
  - Requesting removal of infringing content
    - All major social media platforms have procedures in place for users to request removal of infringing content (e.g., by filing a DMCA takedown notice for copyright infringement or a notice of trademark or IP infringement).
  - Filing a complaint
  - In determining your response, consider:
    - What the social media platform requires you to show to support a request to takedown/transfer
      - Twitter requires the complaining party to show a clear intent to mislead, which often makes taking down personal handles significantly more difficult.
    - How notifying the platform and/or the infringing user will affect your ultimate enforcement strategy

Monitoring and Addressing Third-Party Use of Your IP

- Tips:
  - Secure your brand names and trademarks on all major social media sites.
  - Monitor infringing usernames/handles.
    - Assess the costs and benefits to determine whether to take action (even if infringement is not presently harmful).
  - Investigate whether corresponding handles, usernames, etc. are available before you launch a new brand.

Striking the Right Balance

- Your IP enforcement policy for social media must be tailored to your specific business needs.
  - In determining appropriate action, consider:
    - Whether cognizable harm was done to your brand or IP;
    - Your duty to police and enforce your IP to protect your rights;
    - Any benefit you can derive from the third-party use of your IP; and
    - Possible public perception of your enforcement actions and public relations issues, including alienation of your key demographics.

Striking the Right Balance

- AMC and the Takedown and Restoration of *Mad Men* Twitter Handles – Examples of Negative Public Reaction
  - In summer 2008, individuals not affiliated with AMC created Twitter handles for and tweeted as characters from the AMC drama series *Mad Men* (@_dondraper, @peggyolson, etc.)
  - AMC filed a DMCA takedown notice with Twitter, and Twitter responded by suspending the accounts:

Striking the Right Balance

- AMC and the Takedown and Restoration of *Mad Men* Twitter Handles – Examples of Negative Public Reaction
  - The blogosphere's reaction was quite negative (and directed toward AMC):
    - "What could have been cleverly co-opted and adapted into a subtle viral marketing campaign has now been yanked from the interwaves (most likely by reactionary lawyers, our ad dept suspects), deeply upsetting committed yet attention-deficit Twitterers" – Gawker.com, "*Mad Men's* Twitter-Related Kerfluffle"
  - Days later, the Twitter handles were restored – a move the blogosphere then attributed to AMC's outside web marketing group
    - "See, in Web marketing parlance, the Twitterers assuming the names of Mad Men characters are actually 'brand ambassadors' meant to be cultivated, not thwarted. "Better to embrace the community than negate their efforts," says a Deep Focus spokesman. We agree!" – Business Insider, "Twitter, AMC, Wise Up, Restore 'Mad Men' Accounts."

Striking the Right Balance

- AMC and the Takedown and Restoration of *Mad Men* Twitter Handles – Examples of Negative Public Reaction
  - The reinstated Twitter accounts were active years later.

Striking the Right Balance

- Tips:
  - Determine clear triggers for enforcement:
    - Particularly important brands
    - Offensive content
  - Weigh potential harms against potential benefits, and pick the strategy that will best serve your business.

Privacy

Current Privacy Regime in U.S.

- Sector-specific federal legislation (financial services, health care, and education) and marketing restrictions.
- State laws fill gaps or raise standards (e.g., consumer privacy, breach notification, and data security).
- Industry standards, voluntary codes, and government guidance.
- Various state and federal agencies enforcing privacy laws, including the Federal Trade Commission (FTC), Health and Human Service (HHS), banking regulators, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and State Attorneys General ("AG").

Key Federal Privacy Laws

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act/FACT Act (FCRA)
- Federal Trade Commission Act (FTC Act)
- Children's Online Privacy Protection Act (COPPA)
- Telephone Consumer Protection Act (TCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
- Health Insurance Portability and Accountability Act (HIPAA)

Gramm-Leach-Bliley Act

- GLBA created a federal financial privacy regulatory regime for "financial institutions."
- GLBA requires financial institutions to:
  - provide initial and annual written notices summarizing their information collection, use, and dissemination practices;
  - provide customers with opportunity to optout of having their "nonpublic personal information" be disclosed to unaffiliated third parties (except as otherwise permitted by GLBA); and
  - adopt policies and procedures to maintain the security, confidentiality, and integrity of customer records and data.

Fair Credit Reporting Act

- FCRA regulates consumer reporting agencies, furnishers of information, and users of consumer reports.
- FCRA also regulates sharing of information with affiliates and prohibits affiliates from using certain types of shared information for marketing unless consumer is given notice and the right to opt out of these solicitations.
- FACT Act's Red Flag Rules require policies and procedures to identify patterns, practices, or activities that indicate possibility of identity theft.

Federal Trade Commission Act

- Section 5 of FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce.
- FTC has used Section 5 as basis for enforcement actions in the privacy and data security area.
- Settlements between FTC and investigated companies may establish minimum standards regarding data security and effectively expand beyond the parties involved.
- Many states have similar laws providing State AGs and private plaintiffs with right to enforce.

Other Federal Privacy Laws

- Telephone Consumer Protection Act:
  - Restricts telephone solicitations and the use of auto dialers.
- Children's Online Privacy Protection Act (COPPA):
  - Gives parents control over what websites can collect from kids
  - COPPA rules substantially revised in December 2012
- CAN-SPAM:
  - Establishes requirements for commercial messages, gives recipients the right to stop emails.

Health Insurance Portability and Accountability Act

- Provides individuals with notice and certain rights regarding their protected health information (PHI)
- Limits the use and disclosure of PHI
- Service providers to provide assurances regarding proper use, appropriate disclosure, and appropriate safeguards for PHI
- Implements policies and procedures to protect PHI
- Health Information Technology for Economic and Clinical Health (HITECH) Act requires notice if breach of unsecured PHI

Types of State Privacy Laws

- Privacy, data breach, and security laws:
  - California's SB 1
  - Data breach laws
  - Massachusetts security regulations
- Laws applicable to online and mobile privacy:
  - California Online Privacy Protection Act
  - Laws applicable to employers' and schools' use of social media

State Privacy Laws

- California's SB 1:
  - Similar to GLBA but requires opt-in before third-party sharing
  - Imposes restrictions on affiliate sharing and joint marketing
- Data Breach Laws:
  - No federal data breach law but 46 states and DC have laws requiring notice to consumers in the event there is unauthorized access to, or acquisition of, personal information.
  - Many states do not require notice if the information was encrypted and others excuse notice if misuse not reasonably possible or no material risk of harm to the consumer.

State Privacy Laws

- Massachusetts Security Regulations:
  - Require a written security program
  - Require service provider to implement and maintain appropriate security measures
  - Require encryption of personal information across public networks, wireless networks, and portable devices
- California Online Privacy Protection Act:
  - Websites collecting information must post privacy notice
  - Requires disclosures about tracking consumer's online behavior

Industry Standards, Codes of Conduct, and Voluntary Programs

- Payment Card Industry Data Security Standards (PCI DSS)
- White House Privacy Blueprint
  - Privacy Bill of Rights
  - Multistakeholder process for mobile application disclosures, facial recognition technology, and other areas
- Executive Order on Cybersecurity
- EU/US Safe Harbor
- Direct Marketing Association Guidelines

Litigation

Litigation & Social Media: An Overview

- Social Media in Litigation: New Spins on Old Theories
- Use of Social Media in Class Actions
- Advertisements Through Social Media: False Advertising Pitfalls
- Social Media and Discovery
- Social Media: Preservation and Confidentiality
- Use of Social Media During Trial
- Hacking

Social Media in Litigation: New Spins on Old Theories

- Social Media has given rise to new lawsuits asserting traditional claims:
  - Trademark: Lawsuits involving infringement of recognized trademarks over social media
    - Brandjacking
  - Defamation: Proliferation of social media has provided a new for defamatory content, as user comments are widely visible
    - Reputational damage to businesses can be severe, though difficult to quantify
    - Anti-SLAPP considerations
  - Trade Secret: Has social media eroded traditional protections?

Use of Social Media in Class Actions

- Increasingly, the plaintiffs' bar has turned to social media as a mechanism to recruit potential plaintiffs in class actions.
  - Companies should actively monitor social networking sites to gain insight on:
    - Substance of any potential claims against the company, and strategies to mitigate
    - Possible estimation of the size and scope of the class (and any damages)
    - Identity of potential class members, which can save precious time while investigating the merits of any claim
  - Perceived deficiencies in class settlement perpetuated by social media can delay approval of class settlements.
    - "Virtual" or "viral" class actions

False Advertising Pitfalls

- Social media has given rise to a host of risks (and lawsuits) in the false/deceptive advertising context, primarily from blogs and online reviews, leading to the FTC's update of its Guidelines Concerning Use of Endorsements and Testimonials in Advertising to include social media.
- Three Main Areas of Focus:
  - Endorsements: Must be truthful and not misleading.
  - Testimonials: If the endorser's experience is atypical, results that the consumer can expect to achieve must be disclosed.
  - Gifts: Disclose connections between the endorser and the marketer that would affect how people evaluate the endorsement.

Social Media and Discovery

- Like all discovery, discovery requests for social media material must meet applicable relevancy rules; typically, they must be reasonably calculated to lead to the discovery of admissible evidence.
  - Still, social media can lead to a treasure trove of information.
    - Can be important sources of information when plaintiff claims involve bodily injury or emotional harm.
    - However some courts have rejected "digital fishing expeditions"
  - In assessing exposure in a potential lawsuit, companies must be cognizant of the social media footprint of company executives and employees, because they *will* be discovered.
    - Related privilege concerns

Social Media: Preservation and Confidentiality

- Preservation
  - A party's preservation obligations extend to information hosted on social media platforms.
    - What about social media information of employees?
  - Some courts have recognized that preservation obligations create a strain with the fluid nature of social media.
  - Social media should be included in litigation hold notices.
- Confidentiality
  - Pay attention to confidentiality provisions, particularly in settlement agreements. Social media can, and has, led to breach of confidentiality.

Use of Social Media During Jury Trials

- Voir Dire - Social media can and should be a powerful tool during jury selection.
  - Insight into a juror's background, employment, and interests are foundational aspects of the jury selection process, and much of this information often can be gleaned through social media.
  - This can also help identify potential conflicts of interest or bias
    - This can help avoid mistrial
- During Trial – Jurors are prohibited from communicating concerning the trial while it is taking place, and are instructed accordingly. Violations still occur.

We've Been Hacked!

- Even the largest social media operators are subject to hacking; Facebook, Twitter, and LinkedIn have had high-profile attacks.
- Several cases of impersonation have resulted
  - Companies must take steps to ensure that their account information is securely protected, as they would with any other sensitive information.
  - In the event of a successful hack, companies should delete the hacked content, explain the situation and apologize to users, and warn any users if there is a risk of data breach.
  - Liability for hacking?

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

Social Media: Where the Land Mines Are Buried

Eugene Volokh

Gary T. Schwartz Professor of Law, UCLA School of Law
The Volokh Conspiracy, http://washingtonpost.com/news/volokh-conspiracy
Academic Affiliate, Mayer Brown LLP

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Eugene Volokh
volokh@law.ucla.edu
(310) 206-3926

Full First Amendment Protection: Facebook "Like"

- District court:
  - "[M]erely 'liking' a Facebook page is insufficient speech to merit constitutional protection ... .
  - It is not the kind of substantive statement that has previously warranted constitutional protection."

- 4th Cir. (*Bland v. Roberts*):
  - "[C]licking on the 'like' button literally causes to be published the statement that the User 'likes' something, which is itself a substantive statement ... .
  - Aside from the fact that liking the Campaign Page constituted pure speech, it also was symbolic expression[,] ... the universally understood 'thumbs up' symbol ... ."

Full First Amendment Protection: Bloggers Sued for Libel

- District court: "Defendant fails to bring forth any evidence suggestive of her status as a journalist. For example, there is no evidence of

  1. Any education in journalism;
  2. Any credentials or proof of any affiliation with any recognized news entity;
  3. Proof of adherence to journalistic standards such as editing, fact-checking, or disclosures of conflicts of interest;
  4. Keeping notes of conversations and interviews conducted;
  5. Mutual understanding or agreement of confidentiality between the defendant and his/her sources;
  6. Creation of an independent product rather than assembling writings and postings of others; or
  7. Contacting 'the other side' to get both sides of a story.

  Without evidence of this nature, defendant is not 'media.'"

Full First Amendment Protection: Bloggers Sued for Libel

- 9th Cir. *(Obsidian Finance Corp. v. Cox*):
- "As the Supreme Court has accurately warned, a First Amendment distinction between the institutional press and other speakers is unworkable [especially with the advent of the Internet] ... .
- In defamation cases, the public-figure status of a plaintiff and the public importance of the statement at issue—not the identity of the speaker—provide the First Amendment touchstones."

Site Operators Especially Protected

- 47 U.S.C. § 230 protects:
  - Web site operators from liability for commenters' speech;
    - includes corporate blogs;
    - corporate Facebook pages.
  - Web site operators that choose to retransmit speech by others. (*Batzel v. Smith*, 9th Cir. 2003.)
  - Employers sued based on their employees' personal misuse of employer's computer system (*Delfino v. Agilent Tech.*, Cal. Ct. App. 2006).

Doe v. XYC Corp. (N.J. App. 2005)

- XYC's employee posts nude photos of his 10-year-old stepdaughter.
- Stepdaughter sues company.
- Not respondeat superior.
- Negligent entrustment/supervision:
  - "A master is under a duty to exercise reasonable care so to control his servant
  - while acting outside the scope of his employment
  - as to prevent him from intentionally harming others ...
  - if ... the servant ... is using a chattel of the master, and
  - the master ... knows or should know of the necessity and opportunity for exercising such control."
- 47 U.S.C. § 230 not raised.

47 U.S.C. § 230 Exception

- *Roommates.com* (9th Cir. 2008):
  - Roommates required users to enter preferences as to sex, sexual orientation, and family status.
  - "By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others;
  - It becomes the developer, at least in part, of that information."

Business Tweets

- http://www.dailydawdle.com/2012/07/10-hilarious-corporate-business-tweets.html

Business Tweets

Business Press Release

- "Nearly 60 years ago, the legendary test pilot Chuck Yeager broke the sound barrier and achieved Mach 1. Today, [our company] is breaking another kind of barrier with ... ."

Right of Publicity

- It's a tort to:
  - use another's name or likeness
  - without permission
  - for commercial purposes
    - not including news and entertainment
    - but including advertising and merchandising

Employees' Social Media Speech

- Disciplining employee (or perhaps rejecting applicant) based on employee speech may violate statutes in:
  - Cal., Colo., Conn., La., Minn., Mo., Mont., Neb., Nev., N.M., N.Y., N.D., S.C., W. Va.
  - Ordinances in Seattle and Madison.
- More limited protection (focused on partisan politics) in D.C., Ill., Iowa, Wash.
- May even be so if the speech risks disrupting business relationships.

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

Social Media in the Workplace: The Latest Challenges

Charles Broll
VP, GC and Secretary
Nestlé Waters N.A.
203-863-0283
Charles.broll@waters.nestle.com

Katherine Wren
Corporate Counsel
Caterpillar Inc.
wren_katherine_tl@cat.com

Sandra Zubik
Senior Counsel, Labor & Employment Law and Litigation
Hillshire Brands
312-614-7784
sandra.zubik@hillshirebrands.com

Marcia E. Goodman
Partner
Mayer Brown LLP
312-701-7953
mgoodman@mayerbrown.com

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Charles Broll
VP, GC and Secretary
Nestlé Waters North America
charles.broll@waters.nestle.com

Katherine Wren
Corporate Counsel
Caterpillar Inc.
Wren_Katherine_TL@cat.com

Sandra Zubik
Senior Counsel, Labor Relations
Hillshire Brands
sandra.zubik@hillshirebrands.com

Marcia E. Goodman
Partner
Mayer Brown LLP
mgoodman@mayerbrown.com

Social Media Evolution

MAYER·BROWN

Before, During & After Employment

Before Employment

Pre-Employment Screening

- 2013 CareerBuilder survey update -- nearly 39% of employers reported using social networking sites to research candidates.
  - 19% of those employers found information that influenced the decision to ***not*** hire a candidate.
    - Provocative/inappropriate photos
    - Discriminatory comments related to race, gender or religion
  - 43% of those employers found information that factored into the decision ***to*** hire a candidate.
    - Outstanding communication skills
    - Professional-looking profile

Source: http://thehiringsite.careerbuilder.com/2013/07/01/two-in-five-employers-use-social-media-to-screen-candidates/

Pre-Employment Screening

- Employer beware – applicants have protection under discrimination and labor laws BUT ALSO individual state laws, e.g.:
  - New York – consideration of "recreational activities" and legal political activities prohibited.
  - North Dakota – lawful activities outside of work may not be considered.
  - Illinois – use of "lawful products" may not be considered; political affiliation protected.
  - D.C. – political affiliation protected.
  - E.Volokh:http://www.trolp.org/main_pgs/issues/v16n2/Volokh.pdf

Pre-Employment Screening: Password Laws

- Thirteen (13) states already have laws prohibiting employers from requiring applicants & employees to disclose social media passwords:
  - Arkansas
  - California
  - Colorado
  - Illinois
  - Maryland
  - Michigan
  - New Jersey
  - New Mexico
  - Nevada
  - Oregon
  - Utah
  - Vermont
  - Washington
- As of March 1, 2014, legislation is pending in **twenty-three (23) states.**

Pre-Employment Screening: Password Laws

Since mid-2013, more states included exceptions to allow employers to monitor social media accounts in order to comply with other federal or state law or self-regulatory requirements, such as FINRA.

Example: Illinois Right to Privacy in the Workplace Act

Prohibits employers from requesting any employee or prospective employee to provide any password or demand access to the employee's account or profile on a social networking website. 820 ILCS 55/10(b)(1).

Exception:

> "Provided that the password, account information, or access sought by the employer relates to a professional account, and not a personal account, nothing in this subsection shall prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications as required under Illinois insurance laws or federal law or by a self-regulatory organization as defined in Section 3(A)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78(A)(26)." 820 ILCS 55/10 (3.5).

During Employment

Social Media Use Can Have Serious Repercussions

Employees' increasing use of social media – both personal and professional accounts – raises a number of issues.

- Risks (and legal issues) increase because of the speed, broad reach, and permanence of communications on social media.

Social Media Evolution

MAYER·BROWN

BYOD & COPE

- Bring Your Own Device ("BYOD") and social media usage increasingly blur the line between personal life and employment.
- Corporate Owned Personally Enabled ("COPE") is intended to balance corporate security concerns and employee freedom
  - The device (and the corporate data that resides on it) is fully managed and controlled, but also allows for employees to install the apps they like for their personal use.
- Technology is catching up, but challenges remain:
  1. Protecting proprietary company information and trade secrets
  2. Maintaining employee privacy
  3. Ownership of employee creations
  4. Employee activities "outside of work"

BYOD & COPE Policies

Smart Device Policies that Protect Employers

- Have employees agree that:
  - They may be monitored when their device is connected to the work network (and otherwise for business purposes).
  - All device use (including personal) is subject to existing company policies.
  - Company may remotely wipe the device if it is lost, stolen or employment ends.
  - The company may review the device during the exit interview and whenever needed for business purposes.
- Make sure employees understand impact on privacy expectations:
  - Employers may be able to track employee's location.
  - Personal data stored on the device may be erased if the company wipes the data.
  - Employer may access personal data stored on the device.
  - No expectation of privacy – but company may set balance to avoid monitoring of personal information.

BYOD & COPE: Bad Facts make Bad Law

Lazette v. Kulmatycki, et al. (N.D. Ohio 2013)

- After plaintiff left employment and returned her company-issued Blackberry, supervisor read 48,000 e-mails sent to plaintiff's personal Gmail account.
- Plaintiff was unaware that she had left access to Gmail account on device.
- Stored Communications Act (SCA) analyzed in detail; SCA claims could proceed only for e-mails not yet opened.
- Invasion of privacy claim survived motion to dismiss.
- BYOD lessons: common sense helps. Warning about monitoring: no expectation of privacy and employee responsibility helps more.

Social Media Policies

- Policies should provide employees with guidance about the appropriate use of business-related social media accounts, including instructions on how to avoid blurring the lines between company and personal accounts.
- Set forth terms of employee access to company social media accounts and passwords, including procedures to prevent individual employees from changing account usernames or passwords without authorization.
- Be careful not to run afoul of the National Labor Relations Act, state laws restricting employers' access to employees' personal social media accounts, or the applicable social media platforms' terms of use.
- Consider addressing supervisor/management-employee relationships on social media sites.
  - *Stewart v. CUS Nashville, LLC* (No. 3:11-cv-0342, M.D. Tenn., Aug. 8, 2013).
- Make sure policies are crafted to encompass new technologies, e.g., Vine.

NLRB & Social Media Policies

- Potentially **unlawful** restrictions on social media posts:
  - Confidentiality regarding working conditions.
  - Disparaging comments about the employer.
  - Use of company logos.
  - Obtaining management approval before posting.
  - Restricting communication with outside parties.
- Potentially **lawful** restrictions on social media posts:
  - Performance of company's products or services.
  - Privileged or proprietary information.
  - Posts that would violate federal or state law.
  - Posting in the name of the company.

NLRB & Social Media Policies

- NLRB addresses previously open question about "savings clauses" in social media policies:
  - *Giant Food LLC*, NLRB Division of Advice, No. 5-CA-64795, released July 2013: advice memorandum by NLRB Associate General Counsel Barry J. Kearney concluded that the **generic savings clause in an otherwise unlawful policy was insufficient to save the unlawful provisions** because it would not be reasonably interpreted by employees that protected activities were actually protected.
  - Also concluded that Giant Food LLC could include in its social media guidelines a prohibition on employees disparaging its products and services, but could not ban the posting of confidential information or the company's logo or prohibit a video being made on the premises.

NLRB & Social Media Policies

UPMC and SEIU Healthcare Pennsylvania, NLRB ALJ Decision & Order, 06-CA-081896 (April 19, 2013)

- Employer's IT Resources Policy allows *de minimis* personal use of the employer's IT systems, but prohibits participation on websites or social networks (i.e., Face Book, Twitter, etc.) that:
  - describe any affiliation with the employer
  - disparages or misrepresents the employer
  - makes false or misleading statements regarding the employer
  - uses the employer's logos or other copyrighted or trademarked materials.
- Policy also requires approval from the CIO before "sensitive, confidential, and highly confidential information" is transferred over the Internet. "Confidential information" defined to include compensation data, benefits data, staff member data, and policies/procedures.

NLRB & Social Media Policies

UPMC and SEIU Healthcare Pennsylvania, NLRB ALJ Decision & Order, 06-CA-081896 (April 19, 2013)

– Policy violates the NLRA.

- Nothing in the policy indicates that any protected activity is exempt from the rule, and thus, facially, the rule chills Section 7 activity in the absence of a lawfully promulgated rule that draws lines in a nondiscriminatory way explaining which protected conduct is permitted and which is not.
- A rule that does not prohibit using the employer's system for all non-job purposes but rather is reasonably understood to prohibit the expression of certain protected viewpoints (disparaging the employer, misleading statements) and bars use of logos is a prohibition of the expression of certain protected viewpoints that inhibits certain kinds of Section 7 activity while permitting others.
- **Takeaway:** Prohibit all personal use on employer's system? Use examples of what is allowed and what is not allowed? Carefully define "confidential information."

NLRB & Social Media Policies

- In late 2013, Richard F. Griffin, Jr. became the General Counsel for the NLRB.
- In early January 2014, Griffin indicated in an interview with Bloomberg BNA that he "recognized the importance of providing guidance" so that employers can understand and comply with the NLRA
  - Citing Lafe Solomon's mid-2012 advice memorandum on handbook provisions covering Wal-Mart Stores Inc. employees as having "received positive comments."
  - Also citing his own office's November 2013 release about unfair labor practice allegations against Wal-Mart Stores Inc., which he said "gave the employer and employees notice of the NLRB's enforcement of employee rights before the date of the expected activity arrived."
- Griffin had not yet determined how best to provide guidance on employer policy and handbook provisions, but it will be an area the general counsel addresses.

Source: *NLRB Sees an Important Docket and An Active Year Ahead*, 18 DLR S-31, Jan. 28, 2014

Monitoring Employee Social Media Activity

- Many legitimate reasons to monitor
- Monitoring may also help prevent false advertising claims when employees comment on the company or its business.
  - FTC Guideline (16 C.F.R. § 255): liability for failing to disclose material connections with endorsers.
- Monitoring employee social media activity on company time vs. off-duty activity.

NLRB Perspective: Monitoring Employee Activity

- **When is Monitoring Unlawful?** Monitoring employee social media posts is unlawful if the employer has reason to believe that employees are engaging in protected conduct before the monitoring occurs.
- **When is Monitoring Lawful?** Monitoring employees is not unlawful if the protected conduct is reported to the employer by a coworker, as long as the employer has not solicited the information and discloses the source.
- **Note:** Employers are free to observe protected activity by employees in a public area or where employee has no expectation of privacy.

Monitoring: Stored Communications Act

- 18 U.S.C. § 2701 provides punishments for whoever:
  - Intentionally accesses without authorization a facility through which an electronic communication service is provided.
- The Stored Communications Act (SCA) arguably prohibits employers from monitoring employees' online activity without proper authorization or consent.
- Employees may claim that information was gained through misrepresentations or other unlawful means, e.g., ghost accounts.
  - *Pietrylo v. Hillstone Restaurant Group*, 2009 U.S. Dist. Lexis 88702 (D.N.J. 2009) (jury verdict upheld under SCA)

Employee Discipline for Social Media Activity

Laws that played a prominent role in 2013 for employees bringing claims against employers for firings based on social media activity:

- The National Labor Relations Act
- The Stored Communications Act
- Various common law claims, typically invasion of privacy

Employee Discipline for Social Media Activity

National Labor Relations Act

- *Butler Medical Transport LLC* (Nos. 5-CA-97810, 5-CA-94981, 5-CA-97854; Sept. 4, 2013)
  - A social media post does not lose its protection simply because it might have an adverse affect on the company or its business.
  - A post, however, is not protected if it is "maliciously untrue and made with the knowledge that [it was] false."

Employee Discipline for Social Media Activity

National Labor Relations Act

- *Richmond District Neighborhood Center* (No. 20-CA-091748, Oct. 17, 2013)
  - One of the first to show how employees may exceed the protection of the Act on Facebook.
  - A post can be part of concerted activity but could be "so egregious as to take it outside the protection of the Act, or … to render the employee unfit for further service."
- *Bland vs. Roberts* (No. 12-1671, 4th Circuit Court of Appeals, Sept. 18, 2013)
  - Clicking Facebook's "Like" button is speech protected by the First Amendment.
  - Could foreshadow the NLRB's stance on whether "Liking" something on Facebook is protected, concerted activity under the NLRA.

Employee Discipline for Social Media Activity

Stored Communications Act

- *Ehling v. Monmouth-Ocean Hospital Serv. Corp.,* No. 2:11-cv-03305, D.N.J. (Aug. 20, 2013) (granting summary judgment to employer on plaintiff's SCA claim)
  - Court concluded that SCA does apply to Facebook wall posts when a user has limited his or her privacy settings.
  - Here, "authorized user exception" applied because coworker who showed post at issue to management was not coerced into doing so and was intended viewer of the post since he was Facebook friends with the plaintiff.
  - Underscores that employers will lose protection of the "authorized user exception" if they coerce access to Facebook accounts or use other underhanded tactics. NLRB likely to take same approach.

Employee Discipline for Social Media Activity

Stored Communications Act

- *Rodriguez v. Widener University*, No. 13-cv-01336, E.D. Penn. (June 17, 2013) (SCA complaint survives motion to dismiss because no allegations that the post at issue was publicly available).
  - Employee suspended because he was perceived to be a threat to the community based on his Facebook posts displaying images of weapons.
  - Employer claimed it received post from a Facebook friend of the employee, but that did not appear on the face of the complaint and therefore dismissal was improper.
  - Difficult line to walk between employer's duty to investigate and employee's ability to avoid dismissal by not alleging in complaint whether posts were publicly available.

Employee Discipline for Social Media Activity

Common Law Claims

- Invasion of privacy
- Intentional infliction of emotional distress
- Tortious interference

Likely to be a fact-sensitive issue, dependent on the elements of the claim.

Plaintiffs in *Ehling* and *Rodriguez* asserted invasion of privacy claims:

- Ehling's employer won summary judgment on the claim because it did not intentionally intrude into plaintiff's privacy; rather it was the passive recipient of the Facebook post at issue.
- Rodriguez's claim was dismissed because he failed to allege the particular elements of the tort: that his Facebook post was published to the public at large in a way that was highly offensive to a reasonable person or that anyone took knowing or reckless actions that placed him in a false light.

After Employment

Post-Employment Considerations

Ownership disputes over company social media accounts

- Best to establish through agreement/policy
- Factors that courts may assess to determine ownership in absence of agreement:
  - Who set up the accounts and directed the content when the accounts were set up (during or before employment)?
  - Who had access to the accounts and passwords?
  - How was the account associated with the employer's name or brand?
  - The value of the followers, fans or connections?

Post-Employment Considerations

LinkedIn

- What if former employee refuses to update profile to reflect that he or she is no longer employed?
  - *Jefferson Audio Video Sys. Inc. v. Light*, Case No. 3:12-cv-00019, W.D. Ky. (May 8, 2013) (dismissed employer's lawsuit seeking to force former employee to update LinkedIn profile.)
  - Pursue through LinkedIn terms of use?
  - Include requirement in offer letter/separation agreement that employee update all social media accounts to reflect separation within a certain amount of time after termination of employment.
- Carefully consider requests from former employees for LinkedIn endorsements from supervisors or coworkers.

Post-Employment Considerations

Post-Employment Solicitation Through Social Media

- Employers generally have not been successful in challenging a former employee's generic contact of coworkers or customers through social media (e.g., friend "requests" or LinkedIn network request).
- *Pre-Paid Legal Services, Inc. v. Cahill,* Case No. 12-cv-346, E.D. Okla. (Feb. 12, 2013) (court denies injunction to employer who claimed that former employee's Twitter invitations to former coworkers and Facebook posts about his new employer violated non-solicitation agreement).
- Existing contracts and policies may not adequately protect a business from action that can be taken through social networking websites – like public posts on those sites.

Social Media Evidence in Employment Cases

- Information on social media—including the timing and location of posts, tweets, check-ins—provides a window into employees' schedules.
- **Wage/hour litigation:** Social media evidence can be useful in assessing whether employee was on a break or using meal/rest periods.
- Courts permit discovery sometimes but won't allow "fishing expeditions."
  - *E.g.*, *Jewell v. Aaron's, Inc.* (N.D. Ga. July 19, 2013) (citations omitted):
    - Notes that social media "content is neither privileged nor protected by any right of privacy" that would preclude discovery, yet "the Federal Rules do not grant a requesting party a 'generalized right to rummage at will through information that [the user] has limited from public view."
    - Required "a sufficient predicate showing" that plaintiffs were "forced to work through their meal periods."

Social Media Evidence in Employment Cases

- Evidence can be relevant in discrimination cases.
  - *E.g.*, *Giacchetto v. Patchogue-Medford Union Free School Dist*. (E.D.N.Y June 13, 2013):
    - Disability-discrimination claims under ADA and state law:
    - "The fact that Defendant is seeking social network information as opposed to traditional discovery materials does not change the Court's analysis."
    - Emotional distress: "any specific references to the emotional distress [plaintiff] claims she suffered or treatment she received" as well as "any postings on social networking websites that refer to an alternative potential stressor."
    - Facts underlying lawsuit: "Plaintiff is directed to produce … any social networking postings that refer or relate to any of the events alleged" in the complaint.

Social Media Evidence in Employment Cases

- Can employees be on the hook for spoliation of evidence if they fail to preserve social media accounts?
  - *Gatto v. United Air Lines, Inc.* (D. N.J. Mar. 25, 2013):
    - Plaintiff, an employee of another airline injured on the tarmac at JFK Airport, filed a personal injury claim.
    - United sought discovery about injuries from plaintiff's Facebook account, but plaintiff deactivated the account.
    - Magistrate concluded that adverse inference instruction should be given to jury.

Additional Discussion

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

Crisis Mode: Case Studies – What Can be Done? What Should be Done?

Randall Boyce
General Counsel – Foster Farms

Cari Brunelle
Partner – Hellerman Baretz Communications

Lee Soffer
Attorney - Nestlé Waters North America

Carmine Zarlenga
Partner – Mayer Brown LLP

March 11, 2014

The Social Media Evolution

Crisis Mode: Case Studies

Randy Boyce
Senior VP & General Counsel
Foster Frams
randy.boyce@fosterfarms.com

Cari Brunelle
Partner
Hellerman Baretz Communications
cbrunelle@hellermanbaretz.com

Lee Soffer
Attorney
Nestlé Waters
lee.Soffer@waters.nestle.com

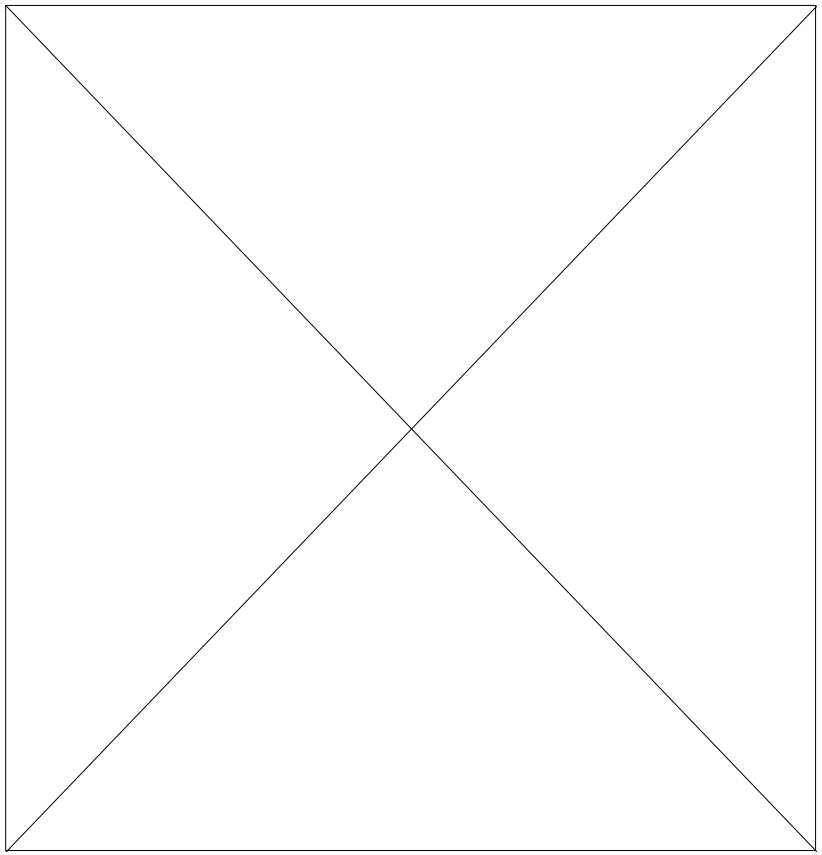
Carmine Zarlenga
Partner
Mayer Brown LLP
czarlenga@mayerbrown.com

Social Media Evolution

MAYER·BROWN

Recent Crisis Situations – Just Plain Dumb

- Fed Ex "Delivery" Gone Wrong
- Abercrombie — CEO
  - "We go after the cool kids"
  - "A lot of people don't belong in our clothes"
- Lululemon — Founder
  - "Some women's bodies… don't work"
  - "Apology" video sparking more outrage.



Social Media Evolution

MAYER·BROWN

Outcomes & Learning – Just Plain Dumb

- Fed Ex Video
  - 9 million views
  - Senior VP Apology video: perfectly executed, resolved issue

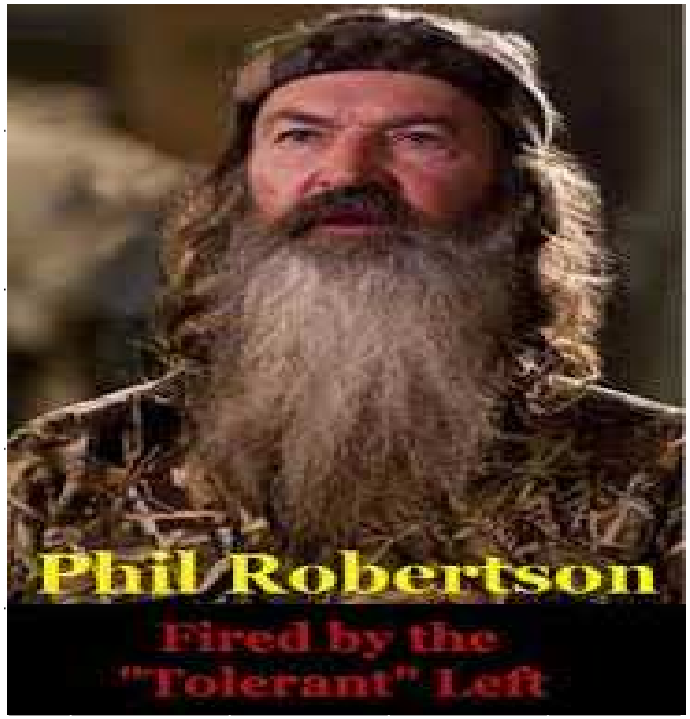
    https://www.youtube.com/watch?feature=player_embedded&v=4ESU_PcqI38
- Abercrombie
  - CEO "apology" note on Facebook, poorly executed, impersonal, prolonged the controversy
  - Revenues and profits in a tailspin (for multiple reasons)
  - CEO contract extended; now selling larger sizes on-line

Outcomes & Learning – Just Plain Dumb *(cont'd)*

- Lululemon
  - Crisis prolonged and long-term damage inflicted
  - Founder Chip Wilson replaced in December
  - Following poor earnings report in January, stock drops 18 percent in one day
  - Company spiraling down and may not recover
- Lesson: Apology will resolve "just plain dumb" crisis. But, must get the apology right.
  - Key Ingredients: (1) apology; (2) sincere regret; (3) corrective action

Crisis Case Study – Offensive and Reprehensible?

- Duck Dynasty "Patriarch" Phil Robertson
  - Homosexuality = sin; see Bible
- Paula Deen
  - At deposition in employment case admitted to using "N word" in the past
- Chick-Fil-A — COO
  - "We are very much supportive of the family – the biblical definition of the family unit"
  - Disappointed with SCOTUS ruling on gay marriage



Outcomes & Learning – Offensive and Reprehensible?

- Duck Dynasty
  - December 18, 2013: A&E issues very soft apology from Phil
  - December 20, 2013: A&E Network "suspends" Phil Robertson
  - Phil support from family and fans "snowballs"
  - December 27, 2013: A&E reinstates Robertson with filming to resume on schedule (and with higher ratings???)
- Lesson: Personal moral beliefs may be controversial, but often can be managed on social media and tolerated.

Outcomes & Learning – Offensive and Reprehensible?

- Paula Deen
  - Food Network fires Deen two days later; numerous endorsement deals cancelled (QVC, Wal-Mart, Home Depot, Sears, Kmart, etc.)
  - Gives rambling and tearful YouTube apology – ineffective
  - Celebrities slowly come to Deen's defense (Oprah, Al Sharpton, Jimmy Carter)
  - Deen cookbook sales escalate; but public image has not recovered
  - Deen wins lawsuit – the white employee that sued has no standing to claim racial discrimination
- Lesson: Social media intolerant of racist behavior; and when "you are the brand" it may be unrecoverable.

Outcomes & Learning – Offensive and Reprehensible?

- Chick-Fil-A
  - July 18, 2012: Media firestorm, heavy attacks
  - July 19, 2012: Very effective Facebook post: "we will treat everyone with honor, dignity and respect . . . our intent is to leave the debate over same-sex marriage to the . . . political arena." [11,000 shares in two weeks]
  - August 1, 2012: Chick-Fil-A "Appreciation Day" per Mike Huckabee proposal — endless lines and record sales at Chick-Fil-A.
  - Record sales for calendar year 2012 (+10%)
- Lesson: Social media counter measures can be very effective; from lemons to lemonade.

Crisis Case Study – Core Competency

- Amy's Baking Co./Kitchen Nightmares on Fox
  - Celebrity Chef Gordon Ramsay is highly critical of Amy's
  - Eccentric owners "go ballistic" with Ramsey and social media naysayers
  - Prolonged and painful social media dialogue

https://www.youtube.com/watch?v=7uPOGxUtZvk&list=PLDiZjlWe4tnt34jE_u_FTddYhOy0mwmak

Social Media Evolution

MAYER·BROWN

Outcomes & Learning – Core Competency

- Amy's Baking Company
  - Social media so overwhelming that owners claim "hacking" occurred; Facebook page shut down
  - Local public relations firm unsuccessful; second Facebook page shut down
  - Restaurant closed temporarily
  - DOL investigation into tip stealing
  - New business: reality show villains
- Lesson: A social media crisis involving the core competency of your business is a problem of the highest order; requires an effective response. Outlash does not work at all.

Crisis Case Study – Human Impact

- Kmart/ Newtown Tweet
  - "Thoughts and prayers to victims"
  - #Fab15Toys

Crisis Case Study – Human Impact

- Kitchen Aid/Obama's GMA
  - Errant tweet from Kitchen Aid employee
  - Tasteless, heartless

Outcomes & Learning – Human Impact

- Kmart/ NewtownTweet
  - Stated that hashtag was unintentional
  - Ended Twitter chat “out of respect for the families”
- Kitchen Aid
  - Issued a textbook apology
  - "During the debate tonight, a member of our Twitter team mistakenly posted an offensive tweet from the KitchenAid handle instead of a personal handle. The tasteless joke in no way represents our values at KitchenAid, and that person won't be tweeting for us anymore. That said, I lead the KitchenAid brand, and I take responsibility for the whole team. I am deeply sorry to President Obama, his family, and the Twitter community for this careless error. Thanks for hearing me out.“
- Lesson: Be very careful with messaging involving human impact. If crisis occurs—retract quickly, with dignity and respect.

The New Crisis Methodology

- Monitor Social Media
- Consider the value in responding
  - Trolls/haters/disrupters: no engagement
  - Blips: limited or no engagement
  - Viral: full engagement
- Define objectives
  - Deny the charge (rarely possible but can be powerful)
  - End the crisis (most common goal) – ant.: Amy's
  - Shift the conversation from negative to positive (the true "value add" – Taco Bell)
- Message design (the hardest part)
- Execution (the tricky part)

Social Media Evolution

MAYER·BROWN

Good Message Design

- Carnival T

- Home Depot

- Taco Bell

Social Media Evolution

MAYER·BROWN

Bad Message Design

- Amy's Baking Co.
- Paula Deen apology
- Abercrombie apology

Special Problems

- The Apology/Admission Problem: No "Magic Bullet"
  - George Zimmerman
  - Foodborne illness
- The Customer Is Wrong Problem: "Hobson's Choice"
  - Under Armour
  - Lululemon

Questions?

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

Social Media and the Corporate Lawyer

Daniel Horwood
Associate General Counsel
Groupon
312-999-3749
dhorwood@groupon.com

Christine Ieuter
Director-Corporate Finance
Allstate
847-402-6840
christine.ieuter@allstate.com

Eddie Best
Partner
Mayer Brown LLP
312-701-7100
ebest@mayerbrown.com

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Daniel Horwood
Groupon
dhorwood@groupon.com

Christine Ieuter
Allstate
christine.ieuter@allstate.com

Eddie Best
Mayer Brown LLP
ebest@mayerbrown.com

Overview

- Traditional and new methods of communicating
- Communicating with the Market
- Insider Trading
- Market Manipulation
- Capital Raising
- Proxy Solicitations
- Social Media and Due Diligence
- General Observations

Traditional And New Methods Of Communicating

- Traditional methods of communicating
  - Offerings
    - Prospectuses
  - Periodic filings
    - 10-Ks, 10-Qs and 8-Ks
  - Communicating with shareholders
    - Annual reports
    - Proxy statements
  - Communicating with the market
    - Press releases

Traditional And New Methods Of Communicating

- New methods of communicating
  - Company website
  - Social media
    - Blogs
    - Twitter
    - Facebook
    - YouTube
    - iPad App

Traditional And New Methods Of Communicating

- Is social media communication advertising or disclosure?
  - Advertising and disclosure are subject to different legal regimes.
  - Some companies have separate social media accounts for different audiences.

Communicating with the Market

- SEC considers "selective disclosure" by public companies to be a form of insider trading.
- Regulation FD (Fair Disclosure) was designed to "level the playing field" and protect market integrity/investor confidence.
- If a public company, or person acting on its behalf, discloses material, non-public information to certain types of recipients, the company must publicly disclose the information:
  - Simultaneously, if disclosure was intentional, or
  - Promptly, if disclosure was not intentional.

Communicating with the Market

- Regulation FD applies only to certain types of speakers at a public company, including employees who regularly communicate with market professionals or security holders.
- Regulation FD applies only to certain types of recipients, including security holders, where the company should foresee that the recipient will buy or sell on the basis of the information, and market professionals.

Communicating with the Market

- Regulation FD applies to material, non-public information.
- Traditional test of materiality:
  - Substantial likelihood that a reasonable investor would consider the information important in making an investment decision.
  - Substantial likelihood that the information would have been viewed by a reasonable investor as having significantly altered the total mix of information.
  - Information that could reasonably be expected to have a substantial effect on the price of the securities.

Communicating with the Market

- Method of disclosure must be reasonably designed to provide broad, non-exclusionary distribution of information to the public.
- The SEC suggests one or more of:
  - Press releases distributed through a widely circulated news or wire service
  - Filings made with the SEC
  - Press conferences or telephonic conferences that members of the public may access (after receiving adequate notice that the conference will be held)
  - Other methods that are reasonably designed to provide broad, non-exclusionary distribution of the information to the public

Communicating with the Market

- Is a mere posting of the material, non-public information on the company website sufficient?
- Is disclosure through other social media outlets sufficient?

Communicating with the Market

- Netflix and New SEC Guidance
  - In July 2012, Netflix's CEO posted a message to his personal Facebook page congratulating company employees on exceeding 1 billion hours of streaming content in the prior month, the first month this threshold had been exceeded.
  - Six months later, the SEC responded by sending a "Wells notice" to Netflix and the CEO, indicating the SEC staff's intent to recommend an enforcement action for violation of Regulation FD.
  - Before the Facebook post, the CEO had publicly stated that the company did not use social media (Facebook or otherwise) to communicate material information to investors.
  - Ultimately, the SEC declined to bring an enforcement action despite some suggestion that it did not consider this particular use of a Facebook post to comply with Regulation FD.

Communicating with the Market

- Netflix and New SEC Guidance
  - The SEC issued a report of investigation affirming that a company may use social media to communicate with investors without violating Regulation FD – **as long as the company had adequately informed the market that material information would be disclosed in this manner.**
  - Whether a company's website or social media disclosure satisfies Regulation FD will depend whether it is considered a "recognized channel of distribution" and whether the public investors are afforded a reasonable period to react to the information.

Regulation FD

- Netflix and New SEC Guidance
  - The SEC cited the following factors:
    - How companies let investors and the markets know to look at the company's web site for information;
    - Whether the company has made investors and the markets aware that it will post important information on its web site;
    - Whether it has a pattern or practice of posting such information on its web site; and
    - Whether the company's web site is designed to lead investors and the market efficiently to information.

Regulation FD

- Netflix and New SEC Guidance
  - The SEC cited the following factors:
    - The extent to which information posted on the web site is regularly picked up by the market and readily available media;
    - The steps the company takes to advise the market of the availability of information on its web site, including the use of "push" technology, such as RSS feeds, or releases through other distribution channels;
    - Whether the company keeps its web site current and accurate; and
    - Whether the company uses other methods in addition to its web site posting to disseminate the information and whether and to what extent those other methods are the predominant methods the company uses to disseminate information.

Regulation FD

- Netflix and New SEC Guidance
  - So what will/should companies do?
  - 2013 NIRI Study found that over half of IROs using social media for IR state that social media postings are held to a lower degree of review than applied to press releases or SEC filings.

Insider Trading

- Under Rule 10b-5 of the Exchange Act and the Insider Trading and Securities Fraud Enforcement Act of 1988, insiders of a corporation may not trade on material, non-public information.
- An "outsider" may be subject to liability if the tippee trades on information that he or she knows or has reason to believe is material, non-public information that was obtained from a corporate insider.

Insider Trading

- Social media provides new opportunities to disseminate material, non-public information or rumors of material events.
- Companies should update their insider trading and confidentiality policies to take account of social media.

Market Manipulation

- Social media can be used to manipulate the market in a company's stock (e.g., false rumors, market manipulation).
- Social media is the perfect place for rumors to grow and eventually impact stock prices.
- Companies have to weigh costs and benefits of responding to false rumors.
- The SEC has announced its intention to investigate false rumor cases.
- Examples:
  - Whole Foods CEO Yahoo message board posts
  - *SEC v. Berliner*

Capital Raising

- Securities Act requires all public offerings to be made pursuant to a registration statement filed with the SEC or an exemption from the registration requirements.
- Offers of securities cannot be made prior to the filing of the registration statement ("gun jumping").
- Written offers can only be made using a statutory prospectus or "free writing prospectus."
- **SEC has stated that statements by electronic means (e.g., postings on websites, e-mails) can be written offers.**

Capital Raising

- Social media communications can run afoul of SEC rules:
  - Gun-Jumping–UBS was removed as a lead underwriter from GM's IPO because of an e-mail sent to potential investors.
  - General Advertising–2011 buyabeercompany.com cease and desist order.
- Companies need to monitor social media communications around an offering to make sure posts are not "offers" of securities.

Capital Raising

- SEC staff, particularly in connection with IPOs, reviews registrant's websites and, presumably, other social media outlets for consistency with prospectus.
- Companies/underwriters must also be careful about responding to blogger's commenting on the offering.

Capital Raising

- Private placements
  - Effective September 2013, new SEC rules eliminated the prohibition under Rule 506 of Regulation D against using general solicitation provided that:
    - all purchasers in the offering are, or are reasonably believed by the issuer to be, accredited investors;
    - the issuer takes reasonable steps to verify their accredited investor status; and
    - certain other conditions in Regulation D are satisfied.

Capital Raising

- Private placements
  - It is still too early to know how extensively social media (e.g., tweets, Facebook messages, etc.) will be used in connection with capital raising.

Proxy Solicitations

- Federal securities laws and regulations regulate the solicitation of proxies.
- Rule 14a-1 defines "solicitation" and "solicit" to include: any "communication to security holders under circumstances reasonably calculated to result in the procurement, withholding, or revocation of a proxy."
  - Example: An issuer puts out a press release announcing a proposed merger and its terms. The release portrays the merger in a favorable light and recommends that securities holders approve the transaction. The press release is a solicitation subject to the proxy rules.

Proxy Solicitations

- Solicitations are subject to a number of requirements, including, in some cases, filing requirements with the SEC.
- Solicitations are also subject to anti-fraud liability.
- Because of the broad definition of proxy solicitation, companies must be careful about corporate communications, including social media posts, around the time of their annual meetings.

Proxy Solicitations

- Subject to some exceptions, a communication by a security holder stating how he intends to vote, and the reasons why, are exempt from the definition of "solicitation."
- This exempt communication can be made on the internet and other social media outlets.
  - Example: CalPERS posts its proxy voting decisions on its Web site (www.calpers-governance.org) approximately two weeks before a company's annual meeting. For each voting issue, it states whether it is for or against the proposal and provides a brief explanation.

Proxy Solicitations

- Companies may find shareholders raising "proxy issues" in social media outlets through exempt communications rather than through traditional proxy process.
- Companies should be careful because their responses to exempt shareholder communications are likely not exempt.

Social Media and Due Diligence

- In connection with both capital raising and M&A transactions, underwriters/buyers will conduct a due diligence review of the issuer/target.
- The growth of the use of social media provides some challenges for traditional due diligence reviews in a number of areas.
- The company's social media policy should be reviewed as well as how the company monitors/enforces the policy.

Social Media and Due Diligence

- Reviewing Public Disclosures
  - In reviewing public disclosures, reviewers must take care to not only review press releases but also companies' websites and social media postings.
  - While reviews have traditionally "looked back" five years, this may or may not be reasonable/feasible with respect to website and social media postings.
  - Reviewers may also want to review social media posts by third parties about the company, as negative comments may provide additional information about the target company's reputation within the market or identify potential "red flags."

Social Media and Due Diligence

- Use of Social Media by Employees
  - Misuse could expose employer to potential liability.
  - Employees could share too much information with the public either about the specific transaction or about the company in general.
  - Employees may post disparaging comments about the company that might affect the underwriters/buyers views.

General Observations

- Adopt and/or update social media policies
  - Policies should work together with code of ethics, insider trading and publicity policies.
- Make sure current insider trading and publicity policies contemplate social media.
- Implement social media education and training.
- Monitor company social media channels.

General Observations

- Be sure IR, Compliance and Legal coordinate.
- Limit the number of authorized speakers.
- Be careful around securities offerings and proxy time.
- Consider process of establishing recognized channel of distribution.
- Have contingency plans in case of leaked information.

General Observations

- When posting:
  - Employ full content and balance.
  - Use or reference disclaimers and forward-looking statement legends.
  - Be carful about linking and re-tweeting third-party content.
  - Don’t forget Reg G for non-GAAP financial measures.

MAYER·BROWN

MAYER·BROWN | Follett | SPOKEO

The Social Media Evolution

The Disruptive Business Practices of Social Media – and its Litigation Risks

John Nadolenco
Partner
Mayer Brown LLP

Laura Corridon
Senior Counsel
Follett Corporation

Angela Saverice-Rohan
General Counsel
Spokeo Inc.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Laura Corridon
Follett Corporation
lcorridon@follett.com

Angela Saverice-Rohan
Spokeo
asaverice-rohan@spokeo.com

John Nadolenco
Mayer Brown LLP
jnadolenco@mayerbrown.com

Litigators Love Social Media

Overview

- Trending social media litigation issues
- New weapon for companies with consumer-facing social media programs?
- Technology and data allowing companies to be more "disruptive."
  - Why are Follett and Spokeo "disruptive"?
  - How to reduce litigation risks?
- Update on current litigation trends.

Social Media Evolution

MAYER·BROWN

Users Demanding Authenticity … and Suing

- ***DiTirro v. Facebook Inc.*** – January 2014 lawsuit over false "likes" in Sponsored Story advertisements on Facebook.

Users Demanding Authenticity … and Suing

- ***DiTirro v. Facebook Inc.*** – Filed a putative class action in N.D. Cal. alleging that Facebook falsely promoted advertisers' pages to other users as having been "liked" by the plaintiffs.
  - Plaintiffs allege they were falsely featured on the Newsfeed as having "liked" pages – such as USA TODAY, Duracell, and Kohl's.
  - Claims for (1) unauthorized misappropriation and commercial use of name, voice, and photographs and (2) invasion of privacy.
  - An amended complaint was filed on January 15, 2014. The case is pending.

Social Media Evolution

MAYER·BROWN

2013 and the Invention of twibel

- Courtney Love was cleared of alleged defamation from a Twitter post.

- ***Gordon & Holmes et al. v. Love*** – Love allegedly defamed a San Diego lawyer through a disparaging tweet that Love says she intended to send as a private message.
- The jury decided that Love did not knowingly make false statements or act with reckless disregard to the truth when she broadcast the tweet in 2010.
- Regular (non-famous) plaintiffs in the past year have also brought Internet defamation claims in state and federal courts around the country.

Review Sites Being Forced to Unmask "Imposters"

- ***Yelp v. Hadeed Carpet Cleaning Inc.*** – Business owner filed suit in Virginia state court against John Doe defendants over allegedly fake Yelp postings. Owner could not match posted dates of service from reviews with real customers.
- Virginia Court of Appeals forced Yelp to disclose reviewer identities, noting that Yelp's terms of service specifically require reviews to be based on actual business patronage.

Disclose "Sponsored" Advertising Posts

- The FTC has used the following guides for endorsements and testimonials in social media advertising since 2009:
  - **Endorsements**: Must be truthful and not misleading.
  - **Testimonials**: If the advertiser doesn't have proof that the endorser's experience represents what consumers will achieve by using the product, the ad must clearly and conspicuously disclose the generally expected results in the depicted circumstances.
  - **Gifts:** If there is a connection between the endorser and the marketer of the product that would affect how people evaluate the endorsement, it should be disclosed.

Tracing the Spectrum of Risk

FTC Target

Safe Practice

Consumer randomly generates positive content for product they purchase

Gifting a free product or something of value to consumer after they randomly generate positive content

Continually giving free products, to the extent that an expectation of future benefits from positive reviews is generated

Blogger receives free product from manufacturer under the condition that he write a review

Advertiser or employee poses as "actual consumer" and posts reviews, commentary, or ratings to discussion boards or websites

Social Media Evolution

MAYER·BROWN

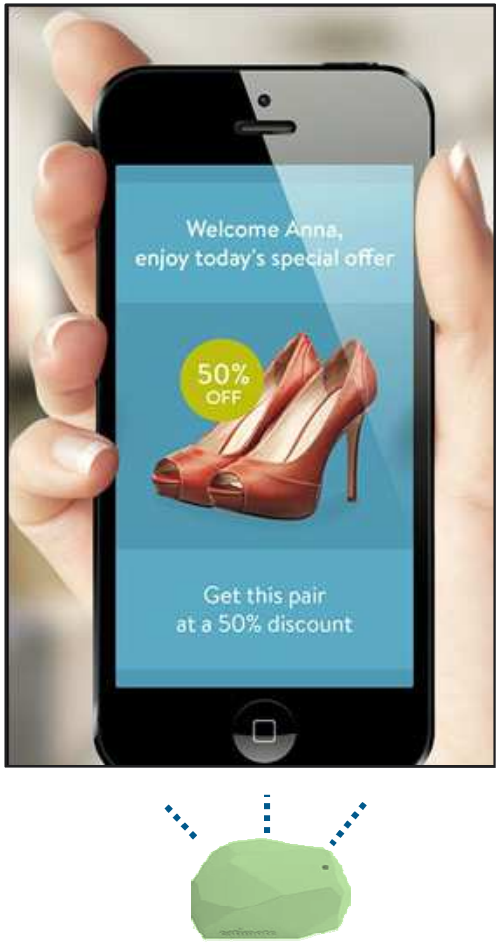
New Mobile Technology, New Risk

- Retailers are looking to engage customers in-store through their smartphones.

Scene from Minority Report (2002)

- Are those retailers "observing" or "tracking" customers?

A Beacon of Opportunity



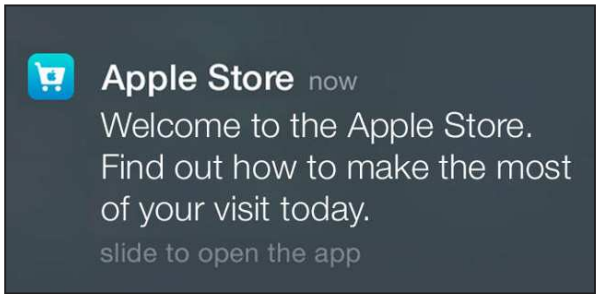
- Many retailers are considering devices equipped with Bluetooth Low Energy (BLE) technology, known as "beacons," in their brick-and-mortar locations.
- Beacons are wireless and serve multiple in-store purposes, such as geolocation, targeted messaging, and retail analytics.
- In-store beacons operate in the background. Guests do not need to open an app to connect.

Social Media Evolution

MAYER·BROWN

Beacon Buy-In from Customers is Key

- 77% of consumers said in a recent survey that they would be willing to share their location data as long as they received enough value in return.



- No set requirements for retailers to obtain customer opt-ins or opt-outs, and there is debate on what should become the industry standards.

- Businesses can avoid litigation by explicitly asking permission at store entry. Disney offers Orlando park guests the option to choose whether to use proprietary wireless "MagicBand" wristbands.

Social Media Evolution

MAYER·BROWN

Privacy Concerns

Sen. Al Franken

- Shopper tracking ignites privacy concerns, particularly given that there are not set disclosure requirements for retailers.
- Beacon analytics companies that provide these services and retailers are pursuing self-regulation under a voluntary code of conduct released in October 2013.
- Sen. Al Franken (D-Minn.) plans to introduce mobile device location tracking legislation.
- Customer tracking remains a ripe area for litigation.

Social Media Evolution

MAYER·BROWN

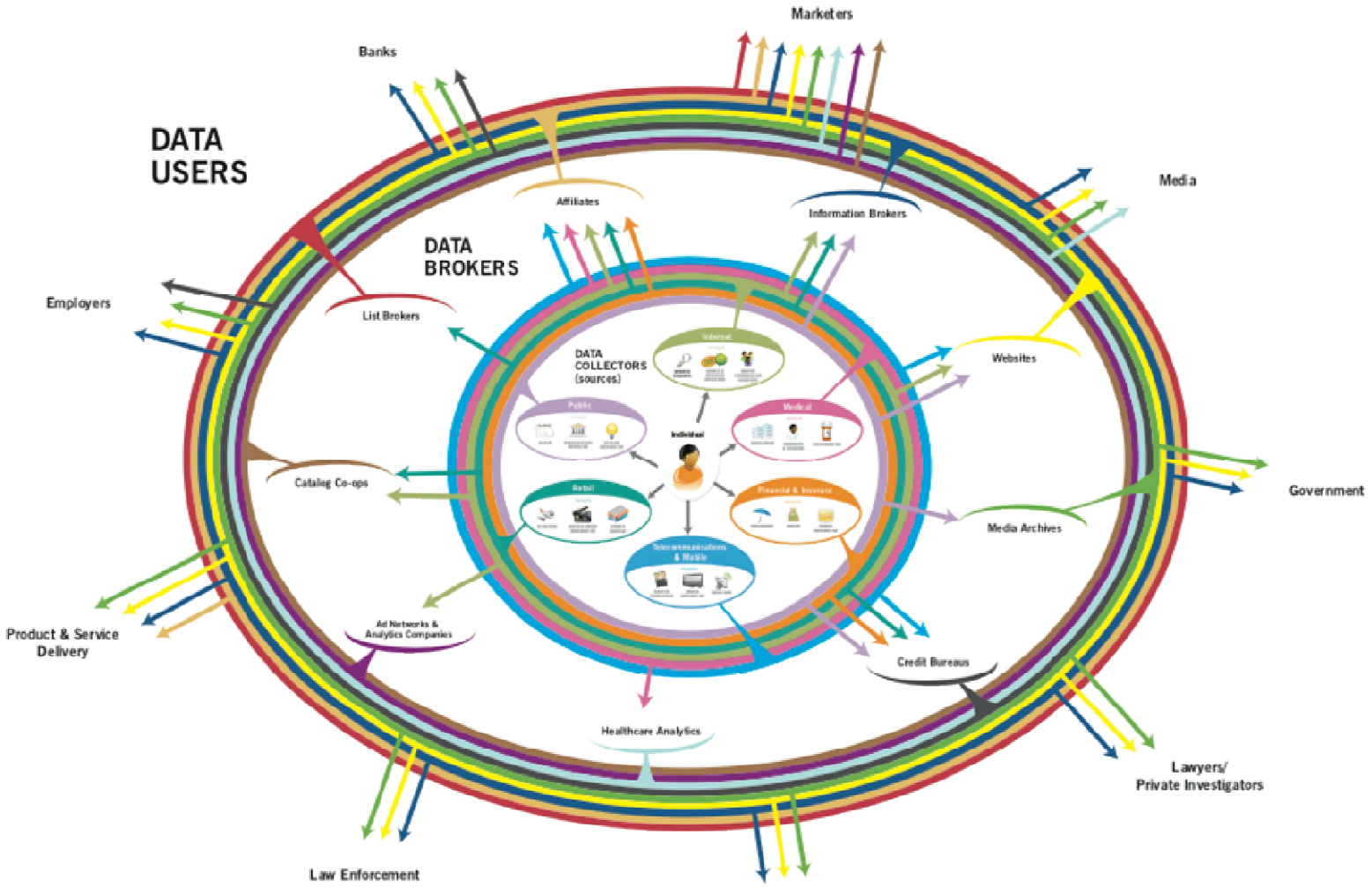
Voluntary Code of Conduct

- The voluntary code of conduct:
  - Asks retailers to post signs in "conspicuous" areas that inform consumers that their movements are being monitored and what site to visit to opt-out.
  - Recommends using the language: "To learn about use of customer location and your choices, visit www.smartstoreprivacy.com."
  - Allows companies to resell the information they collect (for example, to a product manufacturer who wants to know how long customers look at its or a competitor's products).

Browsewrap and Clickwrap User Agreements

- Users accept to "browsewrap" terms through use of site. "Clickwrap" requires an affirmative agreement or click.
- Recent litigation upholding "clickwrap" user agreements demonstrate that a "clickwrap" approach is preferable:
  - ***Hancock v. AT&T*** (10th Cir. 2013)
  - ***In re Online Travel Company Hotel Booking Antitrust Litig.*** (N.D. Tex. 2013)
  - ***Fteja v. Facebook Inc.*** (S.D.N.Y. 2012)

An Expanding Universe of Personal Data



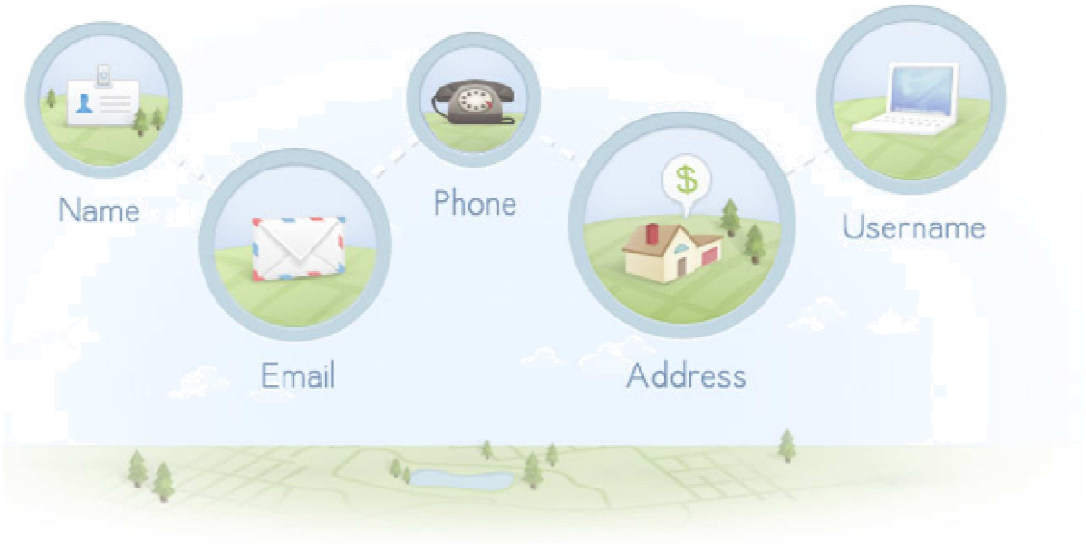
B-2

Social Media Evolution

MAYER·BROWN

The SPOKEO Search Engine

- Spokeo was founded in 2006 by a group of Stanford grads.
- It is a subscription-based people search platform that uses proprietary technology to organize information into comprehensive yet easy-to-understand online profiles.



Increased Scrutiny of Data Brokers

- Recent litigation against data brokers:
  - ***Arcanum Investigations Inc. et al. v. Gordon*** – Plaintiff tried to hold data broker strictly liable for selling DMV records to a stranger who later tracked down and harassed Plaintiff.
- Recent Congressional initiatives:
  - The proposed Data Broker Accountability and Transparency Act would prohibit data brokers from collecting or soliciting consumer information using deceptive means.

Increased FTC Action on Data Brokers

- A Federal Trade Commissioner in a speech in late February asked on Congress to pass laws that would require data brokers to reveal more information to consumers about the privacy of their personal information. Commissioner Julie Brill pushed for the passage of "baseline" laws on commercial privacy, calling for a more aggressive policy for the regulation of personal information in the commercial space.
- FTC completed a report on data brokers in 2013, which is expected to be released soon.

Social Media Evolution

MAYER·BROWN

Article III Standing for Social Media Cases

- Article III standing has remained a hurdle for plaintiffs in social media cases. It has been difficult for plaintiffs to allege – let alone prove – a defendant's alleged conduct caused actual harm. This is starting to change.
- ***Clapper v. Amnesty Int'l USA*** – Last year, the U.S. Supreme Court dealt a serious blow to plaintiffs' ability to seek redress for unauthorized collection of personal information.
- Plaintiffs could not establish injury-in-fact by professing a concern that their connections with foreign terrorists might be targeted for surveillance.

Article III Standing for Social Media Cases

- U.S. District Courts have gone both ways since *Clapper*:
  - ***In re Barnes & Noble Pin Pad Litig.*** (N.D. Ill. 2013) – Citing *Clapper,* the court held that a mere increased risk of identity theft or fraud following hack of credit and debit payment information from PIN pad devices does not constitute actual injury.
  - ***Polanco v. Omnicell*** (D.N.J. 2013) – Similarly, the court cited *Clapper* in rejecting and dismissing plaintiffs' claims regarding a hospital laptop theft. Plaintiff alleged harm from unspecified out-of-pocket expenses from having to visit other facilities where laptops containing personal health information would be better protected.
  - ***In re Hulu Privacy Litigation*** (N.D. Cal. 2013) – A magistrate judge held that a violation of a federal statute providing statutory damages constituted standing regardless of any actual injury.

Potential Game Changer: *Robins v. Spokeo*

- ***Robins v. Spokeo*** (9th Cir. 2014)
  - Facts alleged: Plaintiff was unemployed and alleged concern that incorrect information found by a Spokeo search diminished his employment prospects. Alleged FCRA violation.
  - The District Court dismissed case finding that Plaintiff's concern too attenuated to constitute Article III standing.
  - The Ninth Circuit reversed: "When, as here, the statutory cause of action does not require proof of actual damages, a plaintiff can suffer a violation of the statutory right without suffering actual damages."

Robins Ramifications for Social Media

- The ruling seems inconsistent with *Clapper* and other federal court decisions around the country.
- *Robins* is consistent with new trend in courts allowing Internet privacy cases to proceed beyond pleading stage
- *Charvat* writ petition (was) pending
- Spokeo is considering a petition for certiorari to the U.S. Supreme Court.

Reducing Litigation Risks: Data Breaches

- Hacks and data breaches are a growing priority for both attorneys general and the plaintiffs bar.
  - Data breaches are a constant threat for businesses. Compliance with state notification laws is crucial.
  - California Attorney General Kamala Harris is actively monitoring large data breaches and notifications.
  - ***California v. Kaiser Foundation Health Plan*** – Harris filed and settled claims in January alleging that Kaiser did not timely respond to a data breach. Kaiser waited months before alerting affected individuals. Kaiser agreed to pay a $150K settlement and make data security improvements.

Kamala Harris

KAISER PERMANENTE®

Social Media Evolution

MAYER·BROWN

Watch The Terms of Use

- Apple takes a commission on all digital books (or "iBooks") sold through Apple's iTunes Store.
- Apple changed its terms for in-app book purchases on its devices in 2011, forcing apps to route digital book purchases through its iTunes Store and requiring non-Apple eReader apps to pay the commission.
  - Apple made it clear to outside eReader apps with digital book stores that it intended to enforce these new policies and collect its commission.
- Rather than litigate, most simply removed the sales component in their eReader apps for Apple devices:

  - Google removed its Google Books app from the iTunes Store entirely.
  - Other eReader apps – such as the Nook Kids app and Amazon's Kindle app – stayed on iTunes Store and removed the links within their apps to their own bookstores.

Possible Workaround

- As a workaround, booksellers can possibly sell books without violating Apple's agreement by creating two separate apps for use on Apple iOS devices:

  - A "purchasing app" that enables users to purchase content from an outside website without using the Apple in-app purchase system.
  - A "reader app" that lets users view purchased book content stored locally on the iOS device or through cloud storage.

- However, some of the terms in Apple's agreement are unclear.
- The issue may be clarified through litigation, but so far few eReader app developers have stood their ground against Apple.

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

Anticipating the Risks of Government Enforcement and Private Litigation in Social Media

Jack Halprin
Head of E-Discovery
Google
650-434-2239
jhalprin@google.com

Marcus A. Christian
Partner
Mayer Brown LLP
202-263-3731
mchristian@mayerbrown.com

Archis A. Parasharami
Partner
Mayer Brown LLP
202-263-3328
aparasharami@mayerbrown.com

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Jack Halprin
Google
jhalprin@google.com

Marcus Christian
Mayer Brown LLP
mchristian@mayerbrown.com

Archis Parasharami
Mayer Brown LLP
aparasharami@mayerbrown.com

Following up on Article III Standing

- Is technical statutory violation without showing of actual harm enough? Lower courts are deeply divided.
- Did Congress intend for statutory damages to be multiplied in putative class actions brought on behalf of millions of consumers who have no actual injuries?
- Will Supreme Court intervene?

Government Enforcement

Widespread Use by Individuals and Businesses

- The use of social media has exploded, rocketing from the personal to the professional space and spanning all ages.
- Facebook has more than **1.23 billion** "monthly" active users.
- Proliferation of outlets over the last several years.

Facebook	Twitter	LinkedIn
YouTube	Plaxo	Digg
FourSquare	Vine	Snapchat

Prosecutors And Law Enforcement Are Intensely Interested In All Of This Activity

- Social Networking Providers Publish Data on Government Requests for User Information.
  - *E.g.*, Twitter Transparency Report, Google Transparency Report.
  - Data show government requests are numerous and on the rise.
- In 2009, the DOJ Computer Crime and Intellectual Property Section issued a training document, "Obtaining and Using Evidence from Social Networking Sites."
- Virtually all law enforcement agencies use social media to investigate.
  - NYPD has formed a dedicated unit to mine social media.

Value of Social Media Evidence

- More and more individuals and businesses are publishing more and more statements, photographs, and videos on social media.
- "As long as there have been criminal trials, the best evidence has always been considered to be 'What did the defendant say in his own words.'" William J. Hochul, Jr., U.S. Attorney for W.D.N.Y. *See* USA Today, *Facebook, MySpace social media musings used in court cases* (Aug. 4, 2012).

Value of Social Media Evidence – Government Will Be Able To Collect And Use It

- Privacy no barrier—courts routinely reject notion of expectation of privacy in material posted on social media networks.
  - *See, e.g.*, *Romano v. Steelcase Inc.,* 2010 WL 3703242 (N.Y. Sup. Ct. Sept. 21, 2010); *United States v. Meregildo*, 883 F. Supp. 2d 523 (S.D.N.Y. 2012).
- Some social networking providers may fight subpoenas (not warrants or court orders), but no guarantee that they'll win.
  - *People v. Harris*, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012). Appeal dismissed as moot because Twitter had disclosed user records on pain of contempt. 971 N.Y.S.2d 73 (N.Y. App. Div. 2013).

Value of Social Media Evidence – How It Is Used

- Social media content can be an indicator of fraud (incongruous lifestyle, trips, luxury purchases).
  - Just this year, Facebook evidence was a key part of an indictment against 106 former New York first responders in connection with an extensive Social Security Disability fraud scheme. The scheme dates back to 1988, and as many as 1,000 people are suspected of bilking the federal government out of an estimated $400 million. *See* William K. Rashbum & James C. McKinley Jr., *Charges for 106 in Huge Fraud Over Disability*, N.Y. Times, Jan. 7, 2014, at A1.
  - They were coached on how to fail memory tests, feign panic attacks, and make clear that they could barely leave the house, much less find a job.
  - "But their Facebook pages told investigators a starkly different story." Former police officers claiming disability had posted photographs of themselves fishing, riding motorcycles, driving water scooters, flying helicopters, and playing basketball.

Value of Social Media Evidence – How It Is Used

- Social Media content can also be used to corroborate location and identity.
  - This Instagram photo of a steak and macaroni and cheese dinner, taken at Morton's in Fort Lauderdale, Florida, cited as evidence in aggravated identity theft complaint.
  - Agents were initially unaware of the defendants' identities. The two defendants met cooperating witness at the restaurant and gave the cooperating witness a flash drive containing stolen IDs.
  - From data on the flash drive, agents learned the name of the principal defendant. Agents then found his Instagram profile, which included pictures of himself as well as this steak, which coincided with the meeting.
  - When shown the photos, the cooperating witness identified the defendant as the man who gave him the IDs.

2013, *www.sun-sentinel.com*. (Accessed Feb. 25, 2014).

Social Media Evolution

MAYER·BROWN

Social Media Privacy a Hot Topic for Government Regulators

- The social media dichotomy: Users voluntarily divulge more personal information than ever, but they are also more aware of privacy issues.
- Two Leading enforcement agencies for privacy issues are the Federal Trade Commission and the Consumer Financial Protection Bureau.
- Digital Word-of-Mouth Marketing is huge business – spending expected to top $5 billion in 2015.
- Government agencies will increase scrutiny of how companies use and protect the data they collect online and through social media.

Federal Trade Commission – Data Breach and Behavioral Advertising

- FTC refers to itself as the "top cop on the consumer data security and privacy beat."
- FTC has pursued numerous privacy enforcement actions against social networking providers and other companies.
  - *See, e.g.,* Complaint, Twitter, Inc., FTC File No. 092 3093 (June 24, 2010) (alleged failure to safeguard user information); Complaint, Facebook, Inc., FTC File No. 092 3184 (Nov. 29, 2011) (alleged disclosure of PII to third parties).
  - Many companies settle, but Wyndham Hotels is currently litigating whether FTC has the authority under section 5 to regulate data security. Motion to Dismiss, *FTC v. Wyndham Worldwide Corp.*, No. 13-cv-1887 (D.N.J. filed Apr. 26, 2013).

FTC – Children's Online Privacy Protection Act

- FTC enforces the statute, which regulates collection of personal information from children under 13.
  - *See, e.g.*, *United States v. RockYou, Inc.*, No. 12-cv-1487 (Mar. 26, 2012).
- Not just for websites or online services directed at children; any site or service directed to a general audience is covered if "actual knowledge" that personal information from a child is being collected.
- FTC updated COPPA Rule in 2013 to reflect social media use and other changes in technology; expect additional enforcement.

FTC and Consumer Financial Protection Bureau – Debt Collection and Social Media

- Debt collection is the number two source of consumer complaints to the FTC.
- FTC has applied the Fair Debt Collections Practices Act to social media activity of debt collectors.
  - *See, e.g.*, Letter re: Gary D. Nitzkin, P.C. and Gary D. Nitzkin, 2011 WL 895750 (Mar. 10, 2011) (FTC alleged that Facebook "friend request" sent by debt collection attorney without required disclosures violated statute but declined to pursue enforcement action).
- But the FTC is not the only game in town. . . .

Debt Collection and Social Media

- Consumer Financial Protection Bureau will look to use Dodd-Frank to apply the FDCPA to all creditors, not just third-party debt collectors.
  - *See, e.g.*, CFPB Bulletin, *Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts*, July 10, 2013.
- Advance Notice of Proposed Rulemaking Issued in November 2013.
  - Requests for public comment ask for input on "the use of modern communication channels" in debt collection.

What Does The Future Hold?

- Increased use of social media content by prosecutors in corporate fraud and other white collar criminal cases.
  - Courts' continued resistance to any expectation of privacy in social media content.
- Updated regulation and increased enforcement in the privacy arena by the FTC and CFPB.
  - As hacks and other cyberattacks against companies grow in sophistication, scope, and damage, expect the FTC to continue to investigate companies' security measures and privacy policies aggressively.
  - Will Congress get involved? Data breach legislation proposed in the wake of high-profile incidents (Target, Neiman Marcus).

Private Class Action Litigation

The Plaintiffs' Bar Is Also Intensely Interested

- Privacy more than just a hot topic in the news; plaintiffs' bar has seen an opportunity in "big data."
- Explosion of privacy class actions beginning in 2010 – in large part due to increased attention by FTC to data privacy and voluntary disclosure of PII.
  - Enforcement actions got the ball rolling on consumer internet privacy issues. *E.g., In re Sears Holdings Mgmt. Corp.*, FTC File No. 082 3099 (Aug. 31, 2009) (consent order).
- Government investigates, affected company discloses the issue, and privacy class action lawyers pounce.

Pre-Internet Federal Statutes Rammed Into A Web 2.0 World

- There is no social media or online privacy legislation. Instead, plaintiffs' lawyers invoke laws written long ago.
  - Computer Fraud and Abuse Act (1986)
  - Electronic Communications Privacy Act (1986)
    - Title I (Wiretap Act)
    - Title II (Stored Communications Act)
  - Video Privacy Protection Act (1988)
  - Fair Debt Collections Practices Act (1977)
  - Telephone Consumer Protection Act (1991)

Pre-Internet Federal Statutes Rammed Into A Web 2.0 World

- Plaintiffs' lawyers find these statutes attractive for several reasons.
  - Federal laws apply nationwide, increasing the possibility of representing a nationwide class.
  - In some jurisdictions, they can avoid Article III standing problems by alleging technical statutory violations in the absence of actual injury.
  - These statutes also provide for statutory damages or attorneys' fees (or both), further encouraging plaintiffs' lawyers to file lawsuits despite the fact that actual damages are typically nonexistent.

Current State of Online Privacy Litigation

- Data breach cases have been and will remain popular.
  - Companies facing pending lawsuits include:
    - Target
    - Sony
    - Neiman Marcus
    - Wyndham Hotels
  - Despite a lack of relevant statutes, plaintiffs see large targets and easy complaints to file on the back of FTC investigations, congressional hearings, news reports, and company disclosures.
- Plaintiffs' bar seeks to bring parallel lawsuits in context of social media because those communications involve large quantities of user data.
  - *See, e.g.*, *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013).

Current State of Online Privacy Litigation

- Plaintiffs' bar panning for gold in attacking companies' collection and sharing of PII.
  - Seventh Circuit's denial of Rule 23(f) relief in massive comScore privacy class action (10 million+ potential class members) will further encourage class actions under federal statutes providing for statutory damages. *See Harris v. comScore, Inc.*, 292 F.R.D. 579 (N.D. Ill. Apr. 2, 2013).

Current State of Online Privacy Litigation

- Social media providers are ripe targets for litigation.
  - *See, e.g.*, *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011); *Low v. LinkedIn*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012); *Lane v. Facebook*, 696 F.3d 811 (9th Cir. 2012), *cert. denied sub nom. Marek v. Lane*, 134 S. Ct. 8 (2013) (but will *cy -pres* settlements last?).

- But plaintiffs' lawyers are always looking for new targets. . . .

The Facebook "Beacon" Case – A Beacon for The Future?

- Beacon = a now-defunct partnership between Facebook and dozens of companies that sent data from those companies' external websites to Facebook for advertising purposes and to allow users to share their other internet activities with friends on Facebook.
  - Facebook wasn't the only defendant named in the suit; the complaint named as defendants Blockbuster, Fandango, Hotwire, STA Travel, Overstock.com, Zappos, Gamefly, and other "John Doe" corporations that had activated the Beacon program. *See* Complaint, *Lane v. Facebook*, 2008 WL 3886402 (N.D. Cal. Filed Aug. 12, 2008).
  - Blockbuster was also sued in a separate class action for its participation in Beacon. *See Harris v. Blockbuster, Inc.*, 622 F. Supp. 2d 396 (N.D. Tex. 2009).

The Facebook "Beacon" Case – A Beacon for The Future?

- Companies should be aware that any future information-sharing partnerships with social media services, while valuable from a marketing perspective, will attract similar attention from the plaintiffs' bar.
  - As will any applications or services that run on social media platforms. *See In re Zynga Privacy Litig.*, 2011 WL 7479170 (N.D. Cal. June 15, 2011).

VPPA – Plaintiffs Going After Corporations for Social Media Integration

- Hulu Litigation one to watch.
  - Hulu sued in 2011 for allegedly doing two things: (1) sending viewing histories and user ID numbers to metrics firms like comScore and Nielsen (without ever matching the two) and (2) integrating Facebook into its website and allowing Facebook users to publish their viewing information to their Facebook pages.
  - In rare victories, plaintiffs, despite no showing of actual injury, survived motion to dismiss and summary judgment. 2013 WL 6773794 (N.D. Cal. Dec. 20, 2013).
    - Statute applies to "video cassette tapes or other similar audio visual materials." 18 U.S.C. § 2710. The court stretched the statute to cover streaming online videos.
    - Statute also provides for $2,500 in damages per violation. There's no way that Congress intended for such damage awards to be multiplied by millions of class members.

VPPA – Examples of Plaintiffs Going After Corporations for Social Media Integration

- States also add fuel to the fire by expanding these federal statutes still further.
  - Michigan's version of the federal VPPA also covers audio cassettes and provides for $5,000 in damages.
  - Naturally, then, a plaintiff brought a putative class action against Pandora under the state statute for allegedly disclosing users' listening histories and related data through Facebook-integrated profiles.
  - The court didn't buy it this time. *See Deacon v. Pandora Media, Inc.*, 2012 WL 4497796 (N.D. Cal. Sept. 28, 2012) (dismissing claims with leave to amend, but remarking that "it is questionable whether Plaintiff will be able to allege the requisite facts to establish a claim").

COPPA Cases – More Examples of Plaintiffs Following The FTC's Lead

- Days after FTC issued its changes to the COPPA rule, plaintiffs' lawyers began filing class action suits.
  - *See, e.g.*, *In re: Nickelodeon Consumer Privacy Litig.*, 949 F. Supp. 2d 1377 (J.P.M.L. 2013) (consolidating six putative class actions for allegedly unlawful tracking of internet and video-viewing activities of children under 13).
  - Because COPPA does not contain a private right of action, the plaintiffs "borrowed" alleged violations of the COPPA rule and recast them as claims under the VPPA and Wiretap Act and under arcane state law theories—e.g., intrusion upon seclusion.

FDCPA – The Plaintiffs' Bar Will Be Watching The CFPB

- Plaintiffs may be able to atomize their lawsuits into numerous smaller class actions in order to avoid the statutory cap on damages.
  - *See LaRocque v. TRS Recovery Servs. Inc.*, 2013 WL 30055 (D. Me. Jan. 2, 2013).
- Plaintiffs' bar likely to see an opportunity in CFPB rulemaking and increased enforcement.
  - Even without private right of action under Dodd-Frank, will look to use FDCPA or "borrow" violations of CFPB's interpretation of Dodd-Frank and recast them as violations of state consumer protection laws (e.g., California's UCL).

TCPA – Social Media Companies Fight Back Against Plaintiffs' Abuses

- Text messages are becoming increasingly integrated with social media use.
  - E.g., Twitter allows users to receive tweets on their cell phones in the form of text messages.
  - As social media use varies in format, so too will plaintiffs look to seemingly ill-fitting statutes like the TCPA to bring class action privacy claims.
  - Is it only a matter of time before plaintiffs sue companies under the TCPA for publishing a tweet or similar message that is delivered to them in the form of a text message?

TCPA – Social Media Companies Fight Back Against Plaintiffs' Abuses

- Despite being San-Francisco based, social media companies Twitter and Path had occasion to root for the Los Angeles Lakers in a text spam class action filed against the team. *See Emanuel v. Los Angeles Lakers, Inc.*, 2013 WL 1719035 (C.D. Cal. Apr. 18, 2013).
  - After plaintiff appealed the dismissal of his case, those companies filed an amicus brief in the 9th Circuit accusing plaintiffs in this and other nuisance TCPA actions of wielding the statute "as an extortionate club in cases it was never meant to cover."

Unresolved Issues In Online Privacy And Social Media Litigation

- Because the sheer size of most of these class actions forces defendants to settle even meritless cases once a class is certified, many questions remain:
  - Is good faith or reasonable care a defense in data breach cases?
  - Does users' assent to a privacy policy that permits sharing of PII bar their claims?
  - Can arbitration agreements channel disputes into fair individual arbitrations instead of class actions?
  - Can statutory minimum damages really be multiplied across millions of internet users?
    - Will courts consider those damages mandatory?
  - Will it take a bankrupting damages award (comScore, Hulu) to force Congress's hand?

What Does The Future Hold?

- Data breach, behavioral advertising, and other online privacy litigation not going away.
- Expect the plaintiffs' bar to closely scrutinize companies' partnerships with or incorporation of social media services, particularly if PII is disclosed or shared.

What Does The Future Hold?

- Plaintiffs will continue to look to extend pre-Internet statutes to companies' use of new technologies and social media.
- Expect the plaintiffs' bar to follow the Government's lead.
- Will Congress step in with updated privacy legislation for a digital age?

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

In-House Responses to Social Media IP Issues: Best Practices and Instructive Cases

Matt Griffin
Senior Counsel
Kraft Foods Group
847-646-4872
matthew.griffin@kraftfoods.com

Jason White
Attorney
General Motors
313-665-7377
jason.l.white@gm.com

Richard Assmus
Partner
Mayer Brown LLP
312-701-8623
rassmus@mayerbrown.com

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Matt Griffin
Kraft Foods Group
matthew.griffin@kraftfoods.com

Jason White
General Motors
jason.l.white@gm.com

Richard Assmus
Mayer Brown LLP
rassmus@mayerbrown.com

Social Media Evolution

MAYER·BROWN

Agenda

- How consumer brands are using social media
- Key IP rights and claims at issue
- What can go wrong
  - We will use an instructive case (filed in 2010 and still going) to discuss best practices
- Social media hypotheticals
  - How to handle the Friday afternoon call from your business client demanding action

Social Media at General Motors

Social Media at General Motors

Social Media at General Motors *(cont.)*

Social Media at General Motors *(cont.)*

Social Media at General Motors *(cont.)*

GM social media stats as of mid-February 2014

- *Chevrolet* Facebook Page Likes: 9,913,454
- *Chevrolet* Twitter Followers: 602,800
- *Corvette* Facebook Page Likes: 1,435,952
- *Cadillac* Facebook Page Likes: 1,632,298
- *Cadillac* Twitter Followers: 187,000
- *Cadillac* Google +1s: 1,441,078
- *Cadillac* YouTube Subscribers: 82,022

Millions of consumer impressions

Social Media Evolution

MAYER·BROWN

Social Media at Kraft Foods

Oscar Mayer Real-time Engagement: Super Bowl Ads

Oscar Mayer @oscarmayer · Feb 2
You know what's better than imaginary puppets? A real life hot dog car.
Expand · Reply · Retweet · Favorite · More

Oscar Mayer @oscarmayer · Feb 2
When you roll in a hot dog-shaped car, slow claps kind of just come with the territory.
Expand · Reply · Retweet · Favorite · More

Oscar Mayer @oscarmayer · Feb 2
Every time the @Wienermobile passes 100,000 miles, a hot dog gets eaten. Also at 100,001. Also at 100,002...
Expand · Reply · Retweet · Favorite · More

Oscar Mayer @oscarmayer · Feb 2
Do it for Dad. #Tweet2Lease the 2014 @Wienermobile and chauffeur him around for eight solid hours of dad jokes. youtube.com/watch?v=asfzMj...
View media · Reply · Retweet · Favorite · More

Oscar Mayer @oscarmayer · Feb 2
We'll see your sexy bull and raise you one hot dog. On wheels. It's the @Wienermobile. Get it?
Expand · Reply · Retweet · Favorite · More

Oscar Mayer @oscarmayer · Feb 2
You'll only see one car today that truly cuts the mustard. #Tweet2Lease the 2014 @Wienermobile. bit.ly/1fCE7OA
View media · Reply · Retweet · Favorite · More

Brand-to-Brand Engagement

HONDA to Mr. Peanut Facebook: Power of the peanut vs. power of the HondaVAC, who will win? You're not on Twitter, but that doesn't mean you can hide from the Honda Odyssey with available HondaVAC. We'll track you down, on Facebook and on the floor.

Honda @Honda · Oct 3
Yes, @Sunchips, crumbs are an unfortunate casualty of deliciousness. We're here to pick up the pieces. pic.twitter.com/ZcAGJDSuh0

View photo · Reply · Retweet · Favorite · More

Mr Peanut @MrPeanut · Oct 1
Can't find me on Twitter? Try @MrPeanut . #PowerOfThePeanut +1. Power of the @Honda VAC - 0.
Expand · Reply · Retweet · Favorite · More

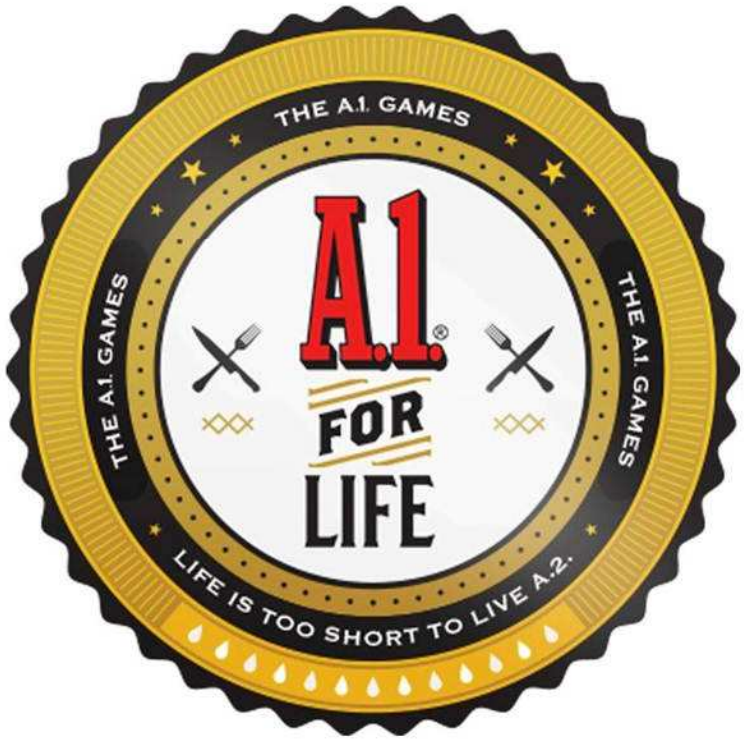
Honda @Honda · Oct 1
.@WONKAnation To you, it's a floor. To me, it's a dining room table. Bring it on little guys. I'm hungry. pic.twitter.com/yNVxSbXeYC

Reply · Retweet · Favorite · More

Honda @Honda · Oct 1
12 great-tasting pieces mean 12 mess-making wrappers @tridentlayers. Until now… --The Honda Odyssey Touring Elite with Built-in HondaVAC.
Expand · Reply · Retweet · Favorite · More

Oscar Mayer + Montaj = User Generated Content

A.1. + Facebook = Enthusiastic Interaction

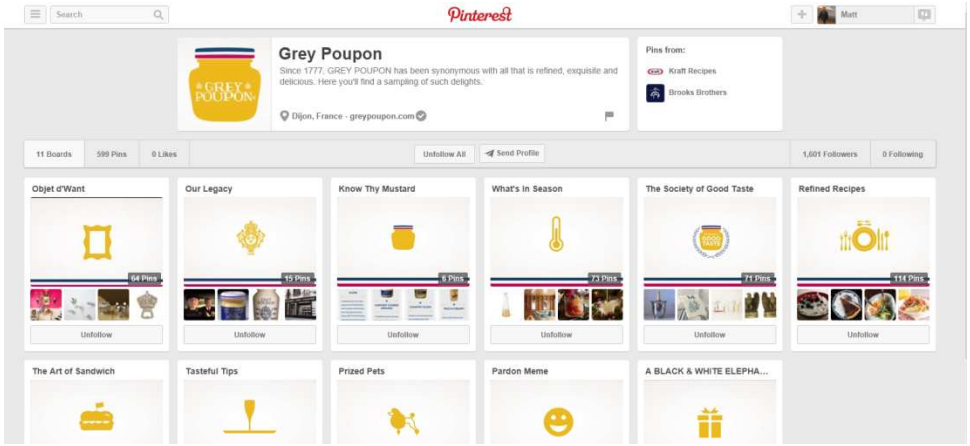


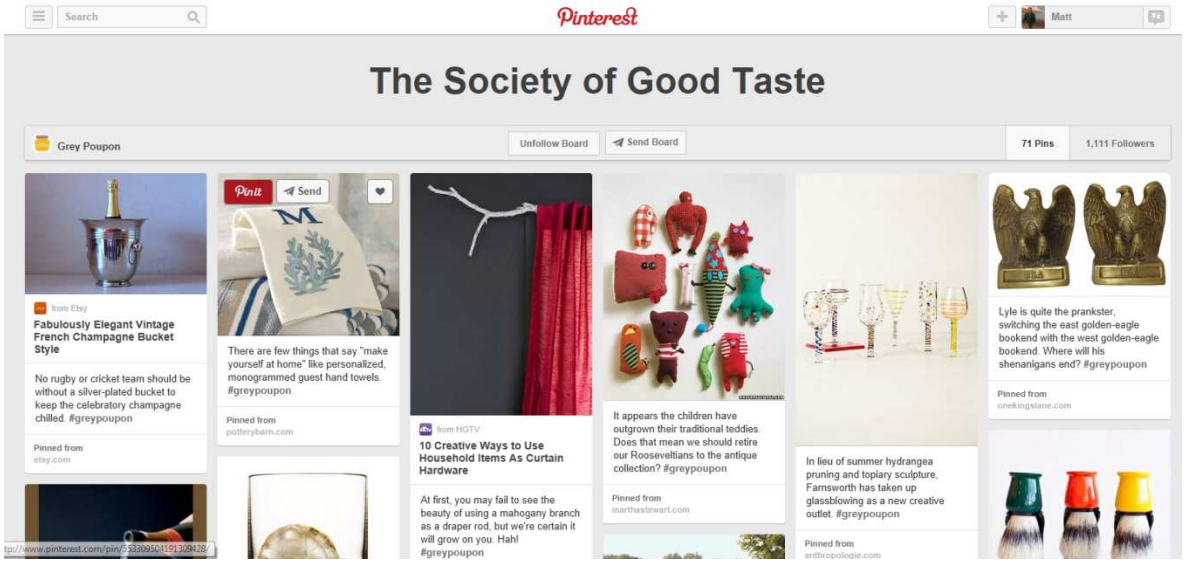
A.1. + Facebook = Enthusiastic Interaction

Social Media Evolution

MAYER·BROWN

Grey Poupon and Pinterest





Development of Intellectual Property Law as Applied to Social Media

Forms of IP/ Claims at Issue in Social Media

Trademarks

- Company names and logos
- Product names and logos
- Taglines

Other Lanham Act claims

- False advertising
- Product disparagement

Other advertising issues

- Undisclosed sponsorships
- Violation of endorsement guidelines

Copyrightable works

- Images
- Text
  - Tweets?
- Music

Publicity rights

- Use of name, photo or likeness
  - Not just celebrities
- Endorsements (actual or implied)

IP Law for Social Media Is 10 Years Behind Internet IP Law

Internet and IP (20 years of experience, cases and statutes)

- 1991 – first website
- 1994 – Yahoo launches
- 1996 – Panavision sues cybersquatter Dennis Toeppen
- 1998 – early metatag lawsuits
- 1998 – DMCA passes
- 1999 – Anti-Cybersquatting Act (ACPA) passes
- 2010 – YouTube DMCA district court decision issues

Social Media and IP (< 10 years)

- 2003 – MySpace launches
- 2004 – Facebook launches
- 2006 – Twitter launches
- 2009 – first defamation lawsuit over a Tweet ("Twible")
- 2009 – Tony La Russa sues over fake Twitter account
- 2010 – Instagram and Pinterest launch
- 2014 – first Twibel jury verdict

Social Media Evolution

MAYER·BROWN

Case Study in Social Media Account Ownership and Use: What Went Wrong?

Social Media Account Ownership and Use

- Many companies have official social media accounts
  - What procedures are in place to control access to those accounts?
- Employees may run their own related social media accounts with an independent following
  - What happens when those accounts are integrated into the employer's social media strategy?
    - Employee's functions carried out through personal accounts
    - Other employer personnel granted access to personal accounts

Maremont v. Susan Fredman Design Group

- Jill Maremont was an interior designer employed by a studio
  - Worked as director of e-commerce, and maintained popular personal Facebook and Twitter accounts related to design
- After accident in 2009, she was off work for months
- Employer was alleged to have access to her Facebook and Twitter accounts
- and to have posted promotions during her convalescence
  - Allegedly did not stop after being asked, and activity stopped only when Maremont changed her passwords

Maremont v. Susan Fredman Design Group (cont.)

- Maremont brought claims for false endorsement under the Lanham Act, violations of her right to publicity and privacy
- On MTD, the N.D. Illinois (772 F. Supp. 2d 967) allowed Lanham Act and publicity claims to go forward:
  - Maremont alleged independent reputation separate from employment sufficient to sustain Lanham Act claims
  - Maremont alleged facts sufficient for social media postings to be considered use of her name and likeness

Maremont v. Susan Fredman Design Group (cont.)

- On the fuller SJ record, the Court dismissed the publicity claims (2011 WL 6101949):
  - Password information for both personal accounts was maintained on employer computers and used by employer personnel with permission
  - Alleged impersonated Facebook postings not of record
  - Tweets did not constitute misappropriation of publicity rights
    - Very first such Tweet was link to website posting about accident and replacement editor for the company blog
    - First Tweet after employee's return thanked her replacements on the blog
  - Employer did not pass itself off as Maremont in the 17 Tweets at issue

Maremont v. Susan Fredman Design Group (cont.)

- Final claim under Lanham Act fully briefed for summary judgment in 2013 and remains pending:
  - Employer argues that because Maremont remained affiliated (employed) by employer during alleged violations, there can be no Lanham Act violation as a matter of law
  - Employer argues that Maremont can show no economic harm
  - Employer argues that Maremont's claims of mental distress from social media posts are not a cognizable form of Lanham Act harm
- Lesson: Even weak claims may result in years of litigation

Hypotheticals (Late on a Friday)

Hypothetical One

You get a call from the head of a very profitable business unit. She just noticed that the unit's newest brand is taken as a Twitter handle. "We want it back, now!" she says.

Hypothetical Two

This same business unit leader calls with another problem, namely a fan blog has just posted about confidential plans for a new product launch. You learn that the fan site has a huge social media presence. "Get a letter out now!" she says.

Hypothetical Three

A different business lead calls. He's sending a marketing team to the Bowl Game (sponsored by your primary competitor), and the team is going to live-Tweet the game, complete with images and Tweets @ the competitor and using the event's coined hashtag. "No problem, right?" he asks.

Hypothetical Four

This time it's the CMO. She noticed that the singer with two chart-topping hits was pictured in a social media post that went viral using the company's new product. "We're going to re-post the picture, and use it in some banner ads. We're also going to Tweet it @ the singer – he has over 2 million followers! We're going to pay him to re-Tweet it. We just need to clear legal this afternoon."

MAYER·BROWN

MAYER·BROWN

The Social Media Evolution

Social Media: Can it have a Role in Internal Investigations without Ethical Sanctions against Company Counsel

Michael Lackey
Partner
Mayer Brown LLP

William Michael
Partner
Mayer Brown LLP

March 11, 2014

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

William Michael Jr.
Chicago
+1 312 701 7653
wmichael@mayerbrown.com

Michael E. Lackey, Jr.
Washington D.C.
+1 202 263 3224
mlackey@mayerbrown.com

Social Media Evolution

MAYER·BROWN

Topics of Discussion Today

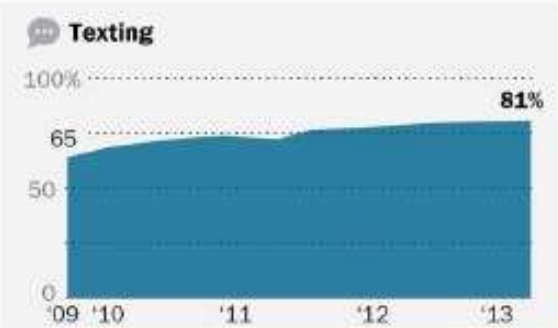
- Statistics and Common Issues involving Social Media
- Access to Individual's Information and the Applicable Legal Framework
  - Corporate vs. Individual Devices
  - Password Protected Information
  - False Accounts
  - Publicly Available Information
- E-Discovery Considerations
  - Discoverability
  - Retention/Duty to Preserve/Spoliation
  - Admissibility

Statistics and Common Issues

Social Media: Who can keep track?

Statistics: Text Messaging

- 91% of adults in the United States own mobile phones.
  - 81% send and receive text messages
  - Nearly a third (31%) prefer texting to calling
- Gen Y are by far the most avid users of text messages.
  - 97% of U.S. adults between 18 and 24 own mobile phone
  - This population sends or receives an average of ***109.5 messages per day***



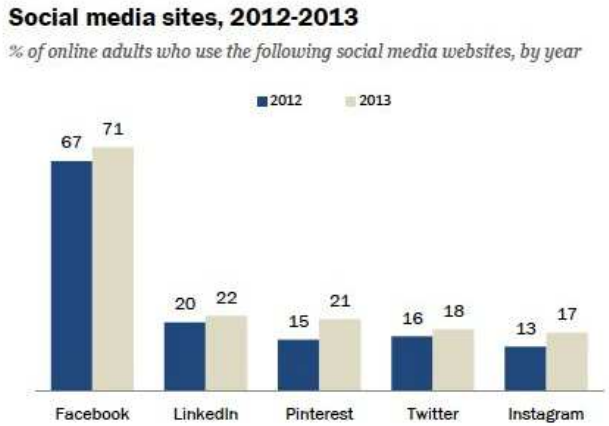
Source: Pew Research, "Cell Phone Activities 2013" (http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/)

Social Media Evolution

MAYER·BROWN

Statistics: Social Media

- 73% of online adults use at least one social networking site:
  - Facebook remains king (71% of online adults), but use of other sites is increasing, chiefly LinkedIn, Pinterest, Twitter, and Instagram.
  - Most Facebook and Instagram users visit those sites at least once a day.



- 90% of Gen Y uses at least one social media platform (esp. Facebook); other groups not far behind.
- **Sources: Pew Research, "Social Networking Fact Sheet" (http:// www.pewinternet.org/fact-sheets/social-networking-fact-sheet/); "Social Media Update 2013" (http://www.pewinternet.org/2013/12/30/social-media-update-2013/)**

What Does This Mean for Employers?

- Young adults entering the workforce bring their communications preferences along with them.
- Content is unpredictable: the conventions and features of e-mail do not apply.
  - Proper use of subject lines
  - Appropriate signatures
  - Automatic spell-check before sending
  - Metadata stripping

- Casual real-time feel + widespread assumption that deletion of texts is irreversible can lead to sticky situations…

Notable Cases

Notable Case: BP/Deepwater Horizon

- BP engineer Kurt Mix deleted more than 500 text messages relating to the April 2010 explosion of the Deepwater Horizon oil rig.
  - Because Mix used a smartphone, federal investigators were able to recover all but 17 of the messages.
  - Contained estimates of oil spill rates up to 3x higher than public disclosures.
  - Forensic methods showed that Mix had deleted the messages 16 months after receiving a legal hold notice for all records, including texts.
- Serious consequences:
  - BP pled guilty to criminal charges and paid $4.5 billion in penalties; largest criminal fine in history.
  - Mix was convicted of obstructing justice in December 2013; faces up to 20 years in jail and $250k in fines.

Notable Case: Fort Lee Traffic Disaster

- Closure of lanes on the NJ side of the George Washington Bridge turned into a still-simmering scandal for NJ Gov. Christie after emails/texts were released:

(Fort Lee Mayor)

Sent 9/10/13 8:04 AM

Sokolich text to Baroni: Presently we have four very busy traffic lanes merging into only one toll booth..... The bigger problem is getting kids to school. Help please. It's maddening

Received 9/10/13 8:05 AM

Is it wrong that I am smiling?

Sent 9/10/13 8:05 AM

No

Received 9/10/13 8:05 AM

I feel badly about the kids

Received 9/10/13 8:06 AM

I guess

Sent 9/10/13 8:11 AM

They are the children of Buono voters

Top Christie Aide

Notable Case: NetFlix CEO Reed Hastings

- On July 3, 2012, Hastings posted on the Netflix Facebook page:
- Stock price jumped 13%
- Resulted in a "Wells notice" – warning that SEC may bring an enforcement action against Netflix for violating Reg FD.

  - Reg FD requires companies to disclose material non-public information to all investors at the same time.
  - Did Netflix violate Reg FD by disclosing this information only to subscribers to the company's Facebook page?
- SEC opted not to sue Netflix; companies now can disclose news through social media "so long as investors have been alerted about which social media will be used to disseminate such information."

Notable Case: Former Congressman Anthony Wiener

Corporate Policies

Corporate Policies – Key Considerations

1. How Texting and Social Media Do – or Do Not – Fit Into the Organization's Business
2. Integration of Policies and Procedures Into Existing Compliance and Supervisory Programs
3. Definition of Social Media
4. Level of Access Employees Have to Social Media on Work Devices During Work Hours
5. Employee Use of Social Media on Personal Devices on Personal Time
6. Level of Company Access to Employee's Work vs. Personal Devices
7. Level of Company Access to Information Stored on Social Media sites

Access & Personal Devices

Bring Your Own Device (BYOD)

- One of the biggest risks presented by employees' bringing their own devices is company data loss.
- Companies can mitigate risks by implementing policies outlining appropriate behavior, usages, and security software for BYOD devices.
- Accessing social media on these privately owned devices presents additional hurdles for the employer: employees have an increased expectation of privacy when using a personally owned device.

Case Study: Text Messages

- If on a work device, employer likely has broad access rights, even to personal messages, especially if illegal or improper activity is suspected.
  - See, e.g., *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010)
  - A California police officer claimed supervisors' search of his text messages violated his Fourth Amendment rights. The officer was using a city-issued pager to send explicit messages.
  - Court found that the City's search was proper, but failed to establish any bright line rules, stating that courts should not use the case to "establish far-reaching premises that define the existence, and extent, of privacy expectations" of workers.

Case Study: Text Messages

- If on a personal device, employers rights will be more limited from a practical and privacy perspective.
  - Internal Investigations: Highly dependent upon cooperation of the employee.
  - Litigation: May need a court order to even obtain the device or data.
  - *Quon* and its progeny indicate that on the balance, the employees right to privacy will be greater on personally owned devices than on work devices.

Access and User Names & Passwords

Employer Requesting Password Access

- Employers have tried to access employee social media by requesting employees to reveal usernames and passwords.
- Varying degrees of coercion: simply ask, stating that participating is voluntary, demand it as a term of hiring or continued employment.
- Restricted by many states, though state-by-state limitations vary.

Employer Requesting Password Access

- Currently, legislation has been enacted or proposed in more than 35 states.
- 12states have enacted laws restricting employer access to employee passwords: Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah and Washington.
- Other states are still developing legislation: New Hampshire, Oklahoma.
- National enforcement challenging, similar to data breach laws.

Employer Requesting Password Access

- Case law also indicates that wholesale access to password-protected information is not allowed by an employer, especially where a policy does not provide as such.
- *Pure Power Boot Camp v. Warrior Fitness Boot Camp* (S.D.N.Y. 2010)
  - The employer's email policy informed employees that the employer could access "any matter stored in, created on, received from, or sent through" the employer's system.
  - The employer obtained the usernames and passwords for the employee's web-based, personal email accounts (i.e., hotmail/gmail) on the employee's work computer and used this information to access the employee's web-based email accounts and read his email.
  - The court found that, where the employee did not actually send or receive the email from the work computer, but merely viewed the email from a work computer, the employer's broad-ranging email policy was not sufficient to prevent the employee from having a reasonable expectation of privacy in the content of his web-based email accounts: "there is nothing in the PPBC policy that even suggests that if an employee simply views a single, personal e-mail from a third party e-mail provider, over PPBC computers, then all of his personal e-mails on whatever personal e-mail accounts he uses, would be subject to inspection."

Employer Requesting Password Access

Pure Power Boot Camp v. Warrior Fitness Boot Camp (S.D.N.Y) (continued)

- Accordingly, the court said that the employee had a reasonable expectation that "his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private" and that the employer's access would be authorized only if the employee had given consent.
- Because the employee had a reasonable expectation of privacy, the employers viewing of the email constituted unauthorized access under the Stored Communication Act, and the employer was prohibited from using the emails as evidence in the underlying labor and employment action between the parties.
- This case, though it pertains to email, is especially applicable to social networks, because all of the communications on social networks is stored on remote servers. An employee may never actually post anything to the social networking site from work, but the employee's username and password might be stored on her work computer.

Employer Requesting Password Access

- See also Electronic Communications Privacy Act (ECP) 18 U.S.C. § 2511
- Whoever "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" commits a violation.
- *Hall v. EarthLink Network, Inc.*
  - EarthLink, an internet service provider, did not violate the ECPA because of a particular exception that was applicable to it as an Internet Service Provider that stored email from the employee as part of its "ordinary course of business."
  - But the Court specifically noted that if a company sets up any mechanism to continually receive and view email transmissions from an employee, the employer likely violates the ECPA, because this is an interception of electronic communications.
  - Thus, if an employer set up a system allowing it to continually monitor email transmissions as they were sent, or social media posts as they were posted, a Court could determine it violated the ECPA.

Shoulder Surfing

- Shoulder surfing refers to the practice of employers asking employees to log onto social media accounts while the employer looks on.
- This happens in the context of hiring , firing, and internal investigations.
- There have been many recent attempts to prevent employers from doing this. In 2012, a number of states including Maryland, California, and Illinois banned this practice.

Keystroke Software

- Keystroke software can be installed on the computer itself, or it can operate remotely through a "Trojan horse" email. In either situation, the information is sent back to the employer for review.
- The software can track application use, log-ons, screen shots, passwords, document tracking, and many other computer activities.
- Keystroke software is directly regulated by some states, and can also fall under some of the other statutes discussed throughout this presentation.

Access & False Accounts

False Accounts: CFAA

- Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030(a)
- Prohibits accessing a computer without authorization.
- An employer who accesses a social networking site surreptitiously – e.g., by assuming a false identity to "friend" an employee on Facebook – may violate the terms of service of the social networking site. An employer may violate the terms of service merely by conducting a background investigation on the site, if the site's terms of service prevent such activity.
- By violating the terms of service of the website, the employer could be deemed to have accessed the "computer" housing the social media website without authorization – technically a violation of the Computer Fraud and Abuse Act (CFAA).

False Accounts: CFAA

- CFAA allows the government to prosecute a criminal violation – unlikely given the breadth of the statute and the low stakes involved for the USAOs.
- However, private plaintiffs can also bring a claim under CFAA, and the language of the statute likely would allow employees to bring a claim: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).
- Thus, by accessing Facebook's website without authorization (i.e., in violation of the terms of service) an employee who claims he/she was harmed as a result could technically bring a claim for a violation of CFAA as a result.

Notable Case: False Accounts & CFAA

- *United States v. Drew*
  - Defendant set up a fake profile on the social networking site MySpace – a practice which violated the site's Terms of Service.
  - The defendant used the fake profile to harass a 13-year-old girl, who committed suicide after the harassment. At trial, the defendant was found guilty of a criminal misdemeanor violation of CFAA, and the defendant then moved for judgment of acquittal.
  - The court held that basing a misdemeanor violation of CFAA solely upon the violation of a website's terms of services is unconstitutional under the void-for-vagueness doctrine. However, the decision leaves open the possibility that a defendant may still face civil penalties under CFAA for violating a website's terms of service.

False Accounts: SCA

Stored Communications Act (SCA) 18 U.S.C. § 2701

- Designed to address access to stored wire and electronic communications and transactional records. "Whoever— (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility."
- The SCA "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." *Theofel v. Farey-Jones,* 341 F.3d 978, 982 (9th Cir. 2003). It "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Id.* at 982.

Notable Case: Access & SCA

Pietrylo v. Hillstone Restaurant Group (D.N.J.)

- Employees set up an invite only website on MySpace.com that criticized their employer.
- The employer asked one of the employees for her username and password to the website, and she provided it. Based on what the employer saw on the website, it terminated some employees.
- Employees sued under the Federal Stored Communications Act, and brought common law claims for invasion of privacy, and wrongful termination among other claims.
- The Court denied the employer's summary judgment motion and set the case for trial, ruling that a jury had to determine whether the employer's mere request for the username and password was coercive, and therefore the employer did not have actual authorization to access the website.

Notable Case: False Accounts & SCA

Pietrylo v. Hillstone Restaurant Group (D.N.J.) (continued)

- A jury ruled that the employer was not properly authorized to access the website under the Stored Communication Act because its request to the employee for her username and password was coercive. This ruling was based solely on the employee's own testimony that she felt that there may have been negative consequences if she did not give her employer her password.
- The Court upheld the jury's verdict in 2009. The employer was held liable for lost wages to the plaintiffs and punitive damages in the amount of four times the lost wages.

Notable Case: Access & SCA

- In 2013, a New Jersey District Court held in *Ehling v. Monmouth-Ocean Hospital* that the SCA applies to Facebook posts.
- Because "the legislative history of the [SCA] suggests that Congress wanted to protect electronic communications that are configured to be private," the court determined that Plaintiff's private Facebook wall post fell under the SCA's protections.
- However, the employer here was not found liable because the post was volunteered by a "friend" of the Plaintiff who had access to the Plaintiff's Facebook posts.

False Accounts:

- Additionally, courts have indicated that employers should not create false social media accounts to circumvent the laws discussed above. Such action may be a violation of the terms of the social media user agreement.
  - *Fteja v. Facebook, Inc.* (S.D.N.Y. 2012) (holding that employers can be civilly liable for violating social media's user agreements)

Access & Public Information

Publicly Available Information

- Publicly available information comes with fewer pitfalls for companies, but care should still be taken when viewing and relying on that information.
- Can be used as evidence of discrimination.
  - *Neiman v. Grange Mutual Casualty Co*.(C.D. Ill. April 26, 2012) (finding evidence that the company used information available on LinkedIn to discriminate against a potential employee based on age).
- Could have confidential information.
  - *See, e.g.,* Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C. § 2000ff-1(a). GINA prohibits employers from obtaining an applicant's "genetic information," defined to include information about an individual's family medical history.
- Should know details of specific social media site.
  - For example, LinkedIn has a feature where can see who has viewed a profile—could raise ethical issues for lawyers, especially if other person is represented.

Ethical Opinions Regarding Lawyers

Relevant Ethical Opinions:

- New York Formal Op. 2010-2 (cannot use false pretenses to obtain evidence)
  - Question Posed: May a lawyer, either directly or through an agent, contact an unrepresented person through a social networking Website and request permission to access their web page to obtain information for use in litigation?
  - Opinion focused on the use of direct or indirect use of affirmatively deceptive behavior to friend a potential witness.
  - Determined that attorney or agent could use truthful information to access social media without also disclosing the reasons for the request.
  - Citing the Ethical Rules (4.1 which forbids knowingly making a false statement), the opinion concluded that the Ethical Rules are violated when the social media contact is made under any type of "false pretenses."

Relevant Ethical Opinions:

- Philadelphia Opinion 2009-02 (ethical rules violated where a third party, at request of a lawyer, sends a connection request)
  - During a deposition a witness indicated they had a Facebook and Myspace account.
  - The request sought third party access by requesting permission from the witness but would not reveal any association with the lawyer nor that they were seeking information for possible impeachment.
  - This was deemed a violation of the ethical rules because the planned communication by the third party with the witness is deceptive. It omits a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness.

E-Discovery Considerations

Uncharted Territory in E-Discovery

- Our digital trails are growing larger and ever more varied
  - Status updates/posts
  - Instant messages
  - Tweets (and retweets)
  - Blogs
  - Photo and video sharing
  - "Follows"
  - "Likes"
  - "Pokes"
  - Comments
  - Groups/causes joined
  - Activity streams
  - Apps downloaded
  - Location "check-ins"

All may qualify as discoverable electronically stored information (ESI) under FRCP 34:

"writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form"

Social Media Evolution

MAYER·BROWN

Uncharted Territory in E-Discovery

- Regulators and litigators are recognizing the potential treasure trove created by text/social media evidence.
- Social Media evidence created by plaintiffs presents opportunities for defendants as well, particularly in class and consumer actions, where discovery obligations typically are imbalanced.
  - *EEOC v. Original Honeybaked Ham* (D. Colo. 2012)
    - EEOC alleged that Defendant had subjected a class of female employees to sexual harassment and retaliation.
    - Defendant sought the contents of class members' email, text messages, and social media accounts.
    - Court agreed that this content was discoverable; privacy concerns over information created for sharing were minimal and could be accommodated by use of a special master and *in camera* review.
- Logistical concern: Widespread use of abbreviations, lingo, and misspellings may make use of search keywords and/or predictive coding difficult.

Notable Case: Consequences

- **HEADLINE: Girl costs father $80,000 with 'SUCK IT' Facebook post.**
- Mr. Snay sued over his departure from Gulliver. A confidential settlement was entered. His daughter then pasted the following on Facebook:
  - *"Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT."*
- A breach of the confidentiality clause was found by the Court and the settlement voided.

Discoverability of Social Media

- *Robinson v. Jones Lang LaSalle Americas, Inc.* (D. Or. 2012)
  - Plaintiff sued for employment discrimination, claiming emotional distress
  - Court ordered production of all of plaintiff's social media communications in any way relevant to "any significant emotion, feeling, or mental state allegedly caused by defendant's conduct" over a 4-year period.
- *Giachetto v. Patchogue-Medford Union Free Sch. Dist.* (E.D.N.Y. 2012)
  - Teacher diagnosed with ADHD sued school district under the ADA and NY State Human Rights Law for discrimination and failure to make adequate accommodations. Defendant moved to compel plaintiff to authorize release of all records from her social networking accounts.
  - Court denied motion as to routine status updates/communications, but agreed that any postings referencing (1) events alleged in the complaint or (2) plaintiff's claimed emotional distress (including other potential sources of distress) were relevant.
  - Plaintiff's counsel was ordered to conduct an independent review of all records for relevance; could not rely on client's assessment.

Duty to Preserve/Spoliation

- Duty to preserve and safeguard all potentially relevant ESI is triggered when litigation filed, threatened, or reasonably foreseeable.
- Courts have not hesitated to impose hefty sanctions or adverse inferences.
- *In re Praxada Product Liability Litigation* (S.D. Ill. 2013)
  - Defendants were sanctioned $931,500 for failing to suspend auto-deletion of text messages between sales force and supervisors.
- *Regas Christou v. Beatport, LLC* (D. Colo. 2013)
  - Defendant issued a legal hold instructing employees to preserve text messages, but did not take steps to collect the data; key defendant lost his iPhone.
  - Court allowed an adverse inference instruction.
- *U.S. v. Suarez* (D.N.J. 2010)
  - Government failed to instruct agents not to delete text messages with a cooperating witness; late litigation hold meant that many of the texts were not preserved on servers/backup tapes.
  - Court allowed an adverse inference instruction.

Retention Considerations

- Critical to establish a routine retention policy (which may, and sometimes should, include a policy that such information is not preserved at all).
- Text messages present data retrieval issues – becomes a balance of importance v. difficulty.
  - Different devices have different storage and backup mechanisms;
  - Readability and length; and
  - Expense – may require extensive forensic work.
- Consider whether company Facebook pages, Twitter feeds, etc. should be archived locally.
  - May save time and money in complying with discovery requests.
  - But keep in mind that the stronger the policy, the more data there is to mine.
- Regulated industries may have particularized retention requirements.

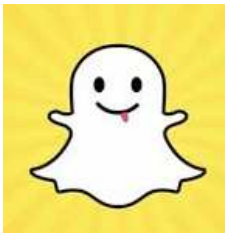
Collection Challenges

- Text and social media ESI present unique complications:
  - Several steps may be needed to produce a record in a useable, understandable format.
  - To minimize time and cost, think ahead:
    - Do you have a collection tool that can be integrated with your e-discovery software?
    - Do you have a method for aggregating content (e.g., a Facebook page) into a usable, understandable format?
    - Do you have a plan for imaging devices (especially if your policy is BYOD)?
    - Is a process in place to document collection decisions and the reasoning behind them?
  - Where will you draw the line about what is "reasonably accessible?"

Collection Challenges

- New technology presents new challenges: "BlackPhone" by Spanish tech company GeeksPhone.
  - Runs an operating system that automatically encrypts emails, text messages and call data.
  - Creates risk for companies with BYOD policies that they will not be able to preserve information relevant to litigation under document preservation procedures.
  - Obtaining relevant information as part of an internal investigation is dependant upon cooperation of the user, which is problematic to the credibility and thoroughness of the investigation.

Self-Destructing Communications



- The wildly popular Snapchat app allows users to share photos that automatically delete after a few seconds of viewing.
  - According to Snapchat, the images disappear from its servers as well.
  - Screenshot capability creates a giant loophole.
  - Message's digital trail is logged (to/from, date, time).

- New Confide app is marketed as Snapchat for business communications.
  - Messages appear in blocked-out format; must swipe to reveal.
  - Once read, messages are destroyed immediately.
  - Alerts sender if a screenshot is taken.
  - Unclear what kind of digital trail is logged.

Social Media Evolution

MAYER·BROWN

Admissibility of Text/Social Media Communications

- The susceptibility of texts/social media to manipulation and falsification creates hurdles to admissibility.
- Authentication issues should be considered from the start.
  - Courts have held that internet printouts are authenticated by witness declaration and circumstantial indicia of authenticity. *Kennerty v. Carrsow-Franklin (In re Carrsow-Franklin)*, 456 B.R. 753, 756–57 (Bankr. D.S.C. 2011).
  - Other methods to consider: data establishing that a particular computer or device was used to create or post the information; requests for admission.
  - Again, documentation of collection/preservation efforts is key.
- Evidentiary case law allows messages to be admissible even absent proof that the message was received, opened or read. Those points go to the weight of the evidence, not admissibility.

Admissibility: What About Hearsay?

- As a general rule, hearsay rules apply to texts and social media just as they do to other evidence
- But little guidance from the courts on how existing hearsay doctrine can be made to accommodate the nature of text and social media evidence:
  - Is a search on WebMD admissible as a "statement made for medical diagnosis or treatment?"
  - Is a text in ALL CAPS an "excited utterance?"
  - Is a status update admissible as a "recorded recollection?"
  - Is a retweet or "like" an "adoptive admission?"
  - Are postings on a company's official Facebook page "business records?"
  - Is a comment on a genealogy website a "statement of personal or family history?"

Summary

- Publicly available information is generally fair game ***with*** parameters.
- False accounts to gain information are not advisable and can lead to sanctions.
- In certain circumstances can get information through passwords and usernames, but weigh the balance of importance against difficulty, and check state statutes.
- Law is adapting in this area slowly to ever changing technology and trending towards the protection of employees' privacy.
- While damages have not yet been significant for violations the risk is that damages will increase.

MAYER·BROWN

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Rich Assmus
Partner | Mayer Brown LLP

Richard Assmus has a balanced intellectual property litigation and transactional practice. He is closely involved in intellectual property due diligence, trademark prosecution and monitoring, copyright counseling and advertising counseling. Richard's dispute resolution experience includes patent litigation, trademark litigation in federal courts and before the US Trademark Trial and Appeal Board, copyright litigation in federal courts and before the Copyright Royalty Board, state court trade secrets litigation, and domain name litigation under the federal anti-cybersquatting act and the UDRP. He also has significant experience advising clients regarding trademark availability; procurement and protection; trademark watch services, including Internet enforcement strategies; copyright protection, registration and enforcement; and negotiating the purchase of domain names.

Edward S. Best
Partner | Mayer Brown LLP

Eddie Best joined Mayer Brown in 1986 and today is co-leader of the firm's Capital Markets group. He is widely recognized as one of the nation's leading capital markets attorneys. Eddie also focuses on corporate transactions, including mergers and acquisitions, involving financial institutions such as insurance companies, banks and brokerage firms. *Chambers Global* calls Eddie "charismatic and intelligent" while *Chambers USA* noted that "[his] 'extremely quick mind' makes him a popular figure among lawyers and clients alike." *Legal500* recommended Eddie in two separate capital markets categories and notes that Eddie is "chief amongst [Mayer Brown's excellent partners]." Eddie has been named a BTI Client All-Star in 2007, 2009 and 2012.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Randall Boyce
Senior Vice President & General Counsel | Foster Farms
Randall Boyce is a lawyer with over thirty years experience in business law. For the past twenty-two years he has worked exclusively within the food industry. After several years with Nestlé USA, Randy became Foster Farms' third General Counsel in 1996. Through a series of acquisitions that began two months after Randy joined Foster Farms, the company has tripled in size and continues to expand its line of food products.

Charles Broll
Vice President, General Counsel & Secretary | Nestlé Waters N.A.
Charlie Broll serves as Vice President, General Counsel and Secretary of Nestlé Waters North America, the third largest non-alcoholic beverage company in the US by volume, with brands such as Poland Spring®, Ice Mountain®, Perrier®, S. Pellegrino® and Nestea®. He previously worked for Diageo Plc, the world's largest beverage alcohol company, in various capacities in Asia, Europe, the Middle East and North America. Prior to going in-house, he was a corporate attorney in Hunton & Williams LLP's offices in New York, Hong Kong and Bangkok, Thailand. Before going to law school, he also worked in Washington, DC as a legislative aide to then-Senator Joe Biden. He holds a JD degree from Duke University.

Cari Brunelle
Partner | Hellerman Baretz Communications
Cari Brunelle is a partner at Hellerman Baretz Communications, an award-winning corporate communications agency for the world's leading law, consulting, healthcare and financial services firms. For the past 15 years, Cari has provided media training and counsel to law firm management and corporate CEOs during high-profile situations. She also served as the media spokesperson on former astronaut Lisa Nowak's case and represented the attorney for both Howard K. Stern and John and Patsy Ramsey. Cari began her career in broadcast news as an anchor and reporter and also produced two documentaries for PBS, one of which was nominated for an Emmy. She spent nearly 10 years in higher education communications and served as the public information officer for a Virginia state agency. Cari was named to Lawdragon's list of "100 Legal Consultants You Need to Know."

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Marcus Christian
Partner | Mayer Brown LLP

Marcus Christian is a Washington DC partner in Mayer Brown's Litigation & Dispute Resolution practice and White Collar Defense & Compliance group. Previously, he was the executive assistant United States attorney at the US Attorney's Office for the Southern District of Florida, the third-highest ranking position in one of America's largest and busiest offices of federal prosecutors. In this role, Marcus worked on the senior management team with responsibility for the Criminal, Civil, Appellate, Asset Forfeiture and Administrative Divisions. During Marcus's career with Southern Florida's US Attorney's Office, he held several roles including serving as a deputy chief in the Major Crimes Section, where he trained and supervised AUSAs, led the Identify Theft and Economic Crimes Task Force and oversaw financial investigations in the Major Crimes Section. As an AUSA, he prosecuted cases involving money laundering, healthcare fraud, mail fraud, wire fraud, national security issues and other matters. Marcus joined Mayer Brown in the fall of 2013.

Laura Corridon
Counsel | Follett Corporation

Laura is counsel of Follett Corporation, a $2.75 billion provider of products, services and software solutions to the educational marketplace from PreK-12 through higher education. Follett operates more than 1,000 college bookstores and delivers physical and digital learning materials and school content and management systems to more than 70,000 primary and secondary schools. At Follett, Laura's responsibilities include trademarks, advertising, marketing, social media, software licensing, joint development agreements and international transactions. Prior to joining Follett, Laura served in the legal departments of several Chicago area companies, including BearingPoint, Inc., Fort James Corporation, Underwriters Laboratories Inc. and Van den Bergh Foods Company.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Anthony J. Diana
Partner | Mayer Brown LLP

Anthony Diana focuses his practice on commercial litigation, electronic discovery, internal and regulatory investigations, and bankruptcies. As a co-leader of Mayer Brown's Electronic Discovery and Records Management group, Anthony has counseled large financial institutions, pharmaceutical companies and manufacturers on all aspects of the discovery and management of electronic information, including: the development of policies and procedures for the preservation, collection, review and production of electronically stored information; the development of data source catalogues, disclosures and responses relating to electronically stored information; the remediation of large volumes of legacy data (paper and electronic); and the defense of electronic discovery procedures before federal regulators and the courts. Anthony is editor of the *Electronic Discovery Deskbook*, a treatise published by PLI, and co-author of six chapters in this treatise. Anthony is a frequent speaker on electronic discovery issues and has published numerous articles on this topic.

Marcia E. Goodman
Partner | Mayer Brown LLP

Marcia Goodman, a partner in Mayer Brown's Chicago office, advises and defends employers on a wide range of employment law matters. She advises employers on access to employee electronic communications and social networking, social media discipline, and employee monitoring advice and disputes. She defends employers in federal class claims regarding discrimination, including hiring criteria and disparate impact claims of race, age, sex, disability and national origin discrimination. She has defended reputation-threatening claims of sexual harassment and retaliation including whistleblower claims. Marcia advises employers in protecting their confidential information from disclosure by current and former employees. Marcia is a contributing author to several publications, including Mayer Brown's *Employee Data Privacy – A Global Overview* in which she provided content related to the United States, Mayer Brown's *The Social Media Revolution: A Legal Handbook*, and PLI's *Securities Investigations: Internal, Civil and Criminal* chapter on Employment Issues in Securities Investigations.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Matthew Griffin
Senior Counsel – Enhancers & Trademark | Kraft Foods Group
Matt represents *Mr. Peanut* and the *Kool-Aid Man*, in that order. He handles trademark, copyright and right-of-publicity matters for Kraft's Beverages business unit (*Crystal Light; Kool-Aid; MiO; Tang; Country Time; Tassimo; Maxwell House; Gevalia*) and its Enhancers and Snack Nuts division (*Planters; CornNuts; Miracle Whip; A.1.; Grey Poupon; Kraft* Mayo, Salad Dressings and Barbecue Sauces), where he also has generalist responsibilities, including advertising review and compliance. He's been involved in real-time social media engagements on behalf of Kraft's *Crystal Light* and *Oscar Mayer* brands during major sporting events and award ceremonies and has helped to develop Kraft's understanding of IP issues related to social media. Prior to Kraft's spinoff from Mondelēz International, Matt worked on the 2012 *Oreo* Daily Twist campaign, which Tweeted visual manipulations of the iconic *Oreo* cookie for 100 daily cultural and historical memes. Matt joined Kraft in 2008. Before that, he was an associate for six years at Pattishall, McAuliffe in Chicago, representing companies in trademark, copyright and unfair competition disputes.

Jack Halprin
Head of eDiscovery, Enterprise | Google, Inc.
As head of eDiscovery, enterprise, at Google, Jack Halprin works to ensure the legal team has the tools, technology and capabilities to ensure discovery obligations are met. He also serves as a member of the team working on the internal records management and information governance program. In addition, he works to build a common strategy across all Google's product lines. Jack speaks frequently on information governance, risk management and compliance at industry events and seminars and has authored numerous articles on eDiscovery, social media, the cloud and knowledge management. He is actively involved in The Sedona Conference and ACC and is a former member of the Electronic Discovery Reference Model (EDRM). His varied expertise lends itself well to both the legal and technical aspects of electronic discovery and information governance. Prior to joining Google in 2012, Jack served as vice president, eDiscovery and compliance, with Autonomy, where he served as a legal subject matter expert and managed the product line strategy for Autonomy's eDiscovery solutions. He has also held various roles with Guidance Software, LexisNexis Applied Discovery and BAR/BRI Bar Review and was a litigation associate at Santa Monica's Haight, Brown & Bonesteel.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Daniel Horwood
Associate General Counsel | Groupon

Daniel Horwood is the Associate General Counsel - Corporate and Securities at Groupon, Inc. where he has spent the last two years, and joined shortly after their IPO. In his role at Groupon, he is responsible for overseeing the company's SEC filings, its acquisitions and joint ventures, and several corporate policies, including FCPA/anti-corruption, insider trading and Regulation FD compliance. He also has responsibility for board of director and board committee matters. He began his career in the SEC's Division of Corporation Finance, where he spent over six years, and his responsibilities included drafting the Securities Offering Reform rules. After the SEC, he moved back to Chicago and spent three years at Mayer Brown's Chicago office, and three years as Senior Counsel at BMO Capital Markets, the investment banking arm of BMO Financial Group.

Christine Ieuter
Director, Corporate Finance | Allstate

Christine Ieuter is the Director of Corporate Finance and Banking at The Allstate Corporation. She specializes in optimizing capital management and company structure to better the efficiency and returns of the organization. In doing this she uses her financial background and love of teaching to communicate in written and verbal ways with stakeholders both inside the organization and externally. After leaving her 7 year career in public accounting that included Ernst & Young LLP and PriceWaterhouse LLP, Christine was the Director of SEC Reporting and Director of Investor Relations for Allstate before taking her current position. Christine is a graduate of Central College of Iowa with a major in Accounting and the University of Illinois – Chicago executive MBA program with an emphasis in marketing. She is a licensed CPA in Illinois and Iowa and a Fellow of the Life Management Institute. She is also a member of the American Institute of Certified Public Accountants and the National Investor Relations Institute, and serves on the advisory boards of Broadridge Investor Communications Solutions and the Economics, Accounting and Management department of Central College. Christine enjoys running, cooking, gardening and restoring her historic home, but most of all spending time with her husband and two daughters. She lives in Wilmette, Illinois.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Michael E. Lackey
Partner | Mayer Brown LLP

Mike Lackey leads Mayer Brown's global litigation and dispute resolution practice. He also serves on the Firm's Partnership Board and co-chairs the Firm's Electronic Discovery and Records Management Practice. Mike is nationally recognized for his knowledge of electronic discovery issues and the impact of social media on litigation. He speaks and writes frequently on these subjects, including co-authoring a forthcoming law review article on "The Ethics of Disguised Identity in Social Media." Mike is a member of the Board of Advisors to the Georgetown University Law School Advanced E-Discovery Institute and of The Sedona Conference®. *Chambers USA* and *Chambers Global* have both recognized him as one of the top E-discovery attorneys nationwide, reporting in 2010 that *"[o]f all the attorneys who do this work, he is a real top gun"* who *"has a good head on his shoulders."* Prior to becoming a lawyer, Mike was a lieutenant in the US Navy and graduated from the "Top Gun" school.

Matthew H. Marmolejo
Partner | Mayer Brown LLP

Matthew Marmolejo is a Litigation & Dispute Resolution partner in Mayer Brown's Los Angeles office. A significant part of Matt's practice centers on representing clients in complex commercial litigation matters with a focus on Latin America. Matt represents both American clients with business disputes in Latin America and Latin American clients involved in US litigation in state and federal courts and in international arbitration proceedings. Matt has conducted comprehensive internal investigations, led extensive pre-trial discovery and motion practice, and has acted as trial counsel for his clients on these matters. In addition to his work in Latin America, Matt takes an interest in the litigation aspects of Social Media. Matt was co-editor of the Second Edition of Mayer Brown's *The Social Media Revolution: A Legal Handbook*, which was released in March 2012. Matt is also a co-editor of the Third Edition of *The Social Media Revolution*, which is scheduled to be released later this year.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

William Michael Jr.
Partner | Mayer Brown LLP
William "Bill" Michael is a partner and Co-Chair of the White Collar Defense & Compliance practice group. He is an experienced trial attorney with more than 100 jury trials in state and federal courts focusing on complex federal white collar and regulatory defense, civil and criminal health care fraud, anti-trust and complex internal investigations. He represents both individuals and corporations in these matters, including: Internal Investigations, Criminal Antitrust, Health Care, Securities Fraud, Criminal Tax, Qui Tams, Money Laundering, Conspiracy and Foreign Corrupt Practices Act (FCPA).

John Nadolenco.
Partner | Mayer Brown LLP
John Nadolenco, a partner in Mayer Brown's Los Angeles office, is an experienced civil litigator whose practice is focused on class-action defense, including defending consumer, securities and employment class actions. John also has experience advising clients on their social media policies, privacy issues and defending clients in privacy-related cases. For example, John is currently representing companies accused of improperly acquiring and tracking user data. John is also advising an application developer whether its practice of sharing information with advertisers violates any applicable laws or website terms of use. John served as co-editor of *The Social Media Revolution: A Legal Handbook*. Prepared by lawyers from across our litigation practices, this handbook provides insight into the risks this developing area presents to business, catalogs the present legal environment related to social media, and offers suggestions for how to proceed.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Archis A. Parasharami
Partner | Mayer Brown LLP

Archis A. Parasharami is a co-chair of the firm's Consumer Litigation & Class Actions practice and a member of the firm's Supreme Court & Appellate practice and Social Media Law task force. Archis is the lead editor of Mayer Brown's Class Defense blog and tweets at *@classdefense*. Archis frequently speaks on developments in the class action arena, and has been quoted on a number of occasions in the *National Law Journal*, *Corporate Counsel* and *The Wall Street Journal*. In 2011, Archis was named by *The National Law Journal* as one of the "Minority 40 Under 40," which identifies minority lawyers who have had significant influence in their practice areas over the past five years. Archis also was named as a Rising Star by *Law360* in the field of class action litigation. He joined Mayer Brown after clerking for Judge Leonard I. Garth of the United States Court of Appeals for the Third Circuit.

Dan Regard
CEO | iDiscovery Solutions

Mr. Daniel L. Regard, CEO and co-founder of Washington, DC based iDiscovery Solutions, Inc. ("iDS"), is a nationally recognized electronic evidence and case management expert with 20 years experience in consulting to legal and corporate entities. A programmer and an attorney by training, Mr. Regard has conducted system investigations, created data collections and managed discovery on some of the highest profile financial investigations of the last decade. He is responsible for the development and implementation of case and matter strategies that leverage technology to clients' best advantage in both litigations and investigations. Mr. Regard has both national and international experience advising on such issues as electronic discovery, computer forensics, database development, application software, data analysis and repository services. He has testified and worked as a testifying expert and as a court-appointed neutral on issues of electronic discovery. Mr. Regard is an active participant in the Sedona Conference's WG1 and WG6 and serves on the Masters Conference Advisory Cabinet. Prior to founding iDS in December 2007, Mr. Regard was the national director of e-Discovery for LECG. He was also the national director of Electronic Evidence & Consulting for FTI Consulting, and was a national leader of Analytical Dispute Services at Deloitte & Touché, where he managed multi-national, multi-

jurisdictional and multi-counsel litigation support projects. He began his career as the founder of a nationwide litigation support practice. Mr. Regard is the founder of b-Discovery, a monthly e-Discovery networking group that meets throughout the United States. He is a director of the Institute of Computer Forensic Professionals and a long-time associate of the Certified Fraud Examiners.

Angela Saverice-Rohan
General Counsel | Spokeo

Lawyer, mother, yogi and lover of social media, Angela Saverice-Rohan enjoys the issues raised at the crossroads of privacy and publicness. Angela is the General Counsel and Chief Privacy Officer for Spokeo, a people search engine based in Southern California. Previously, she served as Associate General Counsel for WellPoint, Inc. where she was responsible for domestic and international privacy and security compliance and served as a key advisor to WellPoint's Technology Division. She has also served as corporate counsel for the global e-commerce company, Digital River, Inc. and Vice President/Corporate Counsel for the Technology and Operations business group at U.S. Bancorp. Through her various roles, she has learned the art of adaptive business counseling, advising a range of clients including sophisticated corporate executives and start up entrepreneurs, in both times of smooth sailing and choppy waters. She obtained a Bachelors of Arts from the University of Minnesota in 1996 and graduated from William Mitchell College of Law in 2002. When she's not busy being a lawyer, Angela may be heard evangelizing on the benefits of sharing via social media, to create a more connected, informed and engaged world.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Lee Soffer
Attorney | Nestlé Waters

Lee Soffer is an attorney working with Nestlé Waters North America (NWNA). Lee provides counsel on all marketing matters regarding NWNA's portfolio of teas and waters. Lee provides support to the brand teams on all social media matters, sweepstakes, contests, partnership agreements and other marketing issues. Prior to working for NWNA, Lee worked with The Coca-Cola Company's Glaceau business unit, providing support for the vitaminwater, smartwater, NOS and Powerade brands and helped streamline the integration of the Glaceau business unit into its parent company. At Glaceau, Lee was responsible for negotiating endorsement agreements and music licensing, and provided legal counsel on all marketing materials. Lee has also worked with a number of startups, small companies and private equity firms in the consumer packaged goods industry, providing legal services for their marketing departments.

Jeffrey P. Taft
Partner | Mayer Brown LLP

Jeffrey Taft is a partner in Mayer Brown's Financial Services Regulatory & Enforcement group based in the Washington, DC office. His practice focuses primarily on privacy and data security, banking regulation, consumer payment systems, consumer financial services and anti-money laundering laws. He has extensive experience counseling financial institutions, merchants and other entities on various federal and state consumer credit protection issues, including compliance with the Gramm-Leach Bliley Act, the Fair Credit Reporting Act, the Electronic Fund Transfer Act, the Right to Financial Privacy Act, state and federal unfair or deceptive practices statutes, telemarketing laws, state privacy and data breach laws and anti-money laundering laws. Jeff regularly assists financial services firms and other companies with their development, implementation and review of privacy and information security programs designed to comply with the Gramm-Leach Bliley Act, state privacy and data breach laws and industry standards, such as the Payment Card Industry Data Security Standards. He also has extensive experience counseling clients on their obligations under federal and state laws in the event of a data breach involving unauthorized access to sensitive consumer information.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Eugene Volokh
Volokh Conspiracy Blog | Washington Post

Eugene Volokh is one of the leading cyberspace law scholars in the U.S.; he has been writing on the subject since his *Cheap Speech and What It Will Do*, published in the *Yale Law Journal* in 1995. He also wrote the leading article on the freedom of speech and information privacy, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop Others from Speaking About You*, published in the *Stanford Law Review* in 2000, as well as the leading article on the free speech rights of private employees (plus about 70 other law review articles and two textbooks). Volokh is also one of the leading law bloggers; he started his *Volokh Conspiracy* blog in 2002, and in early 2014 moved it to the *Washington Post* (http://washpost.com/news/volokh-conspiracy). The blog has been cited over 20 times by courts (Volokh's work more broadly has been cited more than 140 times by courts), and hundreds of times by law review articles. Before going into law teaching, Volokh was one of the leading experts on Hewlett-Packard 3000 computer software.

Jason White
Attorney | General Motors

Jason White is a former Mayer Brown LLP associate with experience in intellectual property counseling and enforcement across a variety of forums, including the U.S. federal courts, the U.S. Trademark Trial and Appeal Board, the National Arbitration Forum and the Federal Trade Commission. He currently serves as an attorney in the Sales & Marketing group of the General Motors Legal Staff, where he primarily focuses on issues relating to global creative content and sponsorship relationships involving GM's various brands. He is a graduate of the University of Michigan and the DePaul University College of Law

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Katherine T. L. Wren
Counsel | Caterpillar Inc.

Katherine T.L. Wren is Corporate Counsel at Caterpillar Inc., representing Electro-Motive Diesel in La Grange, IL. Electro-Motive (owned by Progress Rail Services Corporation, a Caterpillar company) manufactures diesel-electric locomotives and diesel-powered engines. She manages Electro-Motive's employment and labor matters worldwide, and supports commercial transactions for Electro-Motive's locomotive sales. Katherine recently relocated from San Diego, CA, where she provided legal support for Solar Turbines, also a Caterpillar company. Before joining Caterpillar, Katherine was Division Counsel at Wireless Facilities, Inc. She was also Director of Legal for ProfitLine, Inc. In 2012, Katherine was honored with the In-House Attorney of the Year Award by the San Diego Chapter of the Association of Corporate Counsel, having previously received the Chapter's Excellence in Pro Bono Service Award in 2009.

Lori A. Zahalka
Associate | Mayer Brown LLP

Lori Zahalka practices commercial litigation and represents business entities in complex disputes in state and federal courts, including fraud claims, contract disputes and government investigations. She has represented financial institutions against claims brought against them related to their commercial lending activity. She has taken and defended depositions as well as briefed and argued dispositive and discovery-related motions. In addition, Lori practices labor & employment litigation, representing clients in matters before federal and state courts and various administrative agencies, including the defense of individual and class claims of discrimination, wrongful discharge and employment-related torts. Lori also provides clients with counsel and advice on employment-related matters such as employee discipline and termination, employment policies, employment agreements, separation agreements and covenants not to compete. Additionally, she advises employers on emerging issues related to social media in the workplace, including employees' use of social media in the employment context, monitoring of and discipline for employees' social media activity, and post-employment considerations related to account ownership and the application of restrictive covenants to social media activity.

The Social Media Evolution

TRENDS, CHALLENGES & OPPORTUNITIES

Carmine R. Zarlenga
Partner | Mayer Brown LLP

Carmine Zarlenga is a seasoned advocate who has handled a wide variety of complex antitrust, commercial litigation and intellectual property matters. During a career of over 25 years, he has appeared in over 50 different state and federal courts across the United States on behalf of some of the largest national and international companies in the world. Carmine's litigation experience ranges from large, complex class actions with claimed damages in excess of $1 billion and attendant publicity to smaller, private disputes. He often advises clients on media and social media issues that arise in conjunction with high profile litigation and other legal matters and is a frequent public speaker on this topic as well.

Sandra Zubik
Senior Counsel | Labor and Employment, Hillshire Brands

Sandra Zubik has spent much of her legal practice concentrating in the areas of Labor and Employment law. She graduated from the University of Michigan, and received her law degree from John Marshall Law School in Chicago, IL. Her experience includes traditional labor roles, such as negotiating collective bargaining agreements, and handling union organizing campaigns as well as providing advice and direction in employment compliance matters. She is currently Senior Counsel, Labor and Employment and Litigation, for The Hillshire Brands Company (formerly Sara Lee Corporation). Her responsibilities range from providing discharge and discipline recommendations to answering questions about hiring and performance issues. She also supervises all litigation for the company.