



AMERICAN  
BANKRUPTCY  
INSTITUTE

## 2017 Winter Leadership Conference

### **Privacy and Social Media: How It Can Impact Law Firm Security, Ethics and Compensation**

*Hosted by the Ethics, Professional  
Compensation, and Commercial  
and Regulatory Law Committees*

**Janine A. Bowen**

*LeClairRyan, PC; Atlanta*

**Alan L. Friel**

*BakerHostetler LLP; Los Angeles*

**Hon. Bruce A. Harwood**

*U.S. Bankruptcy Court (D. N.H.); Manchester*

**Prof. Lois R. Lupica**

*University of Maine School of Law; Portland, Maine*

**Honorable Bruce A. Harwood**

**U.S. Bankruptcy Court, District of New Hampshire**

**Professor Lois R. Lupica**

**University of Maine School of Law**

**Alan L. Friel**

**Baker Hostetler LLP**

**Janine A. Bowen**

**LeClairRyan, PC**

Privacy and Social Media: How it  
Can Impact Law Firm Security,  
Ethics and Compensation  
American Bankruptcy Institute  
Winter Leadership Conference 2017

1

## Definitions

### “Social Media” or “Social Networking”

- Social media includes any electronic platform through which people may communicate or interact in a public, semi-private or private way. Through blogs, public and private chat rooms, listservs, other online locations, social networks and websites such as Facebook, LinkedIn, Instagram, Twitter, Yelp, Angie's List, Avvo and Lawyers.com, users of social media can share information, messages, e-mail, instant messages, photographs, video, voice or videoconferencing content.
- This definition includes social networks, public and private chat rooms, listservs, and other online locations where attorneys communicate with the public, other attorneys, or clients. Varying degrees of privacy may exist in these online communities as users may have the ability to limit who may see their posted content and who may post content to their pages.
- DC Bar, Ethics Opinion 370

2

# Definitions

## “Social Media” or “Social Networking”

- Enables the sharing of information, ideas, messages, and content using words, photographs, videos and other methods of communication.

{ 3 }

# Definitions

## “Blog”

- Contraction of the term “web log.” Personal (or professional) website where one can upload “posts” and allow comments. Blogs are “new media” because they are DIY media. They can become interactive by allowing reader comments.

{ 4 }

# Definitions

## List-serves

- Connected series of e-mail addresses that allow members of the list-serve to communicate with all the members.
- Most have closed membership (member subject to moderator approval)

[ 5 ]

# Definitions

## **Professional and “Personal” Networking Sites**

- **Linked In:** business orientated social networking site, primarily used for professional networking. Enables people to build, maintain and track professional contacts. Used as a means of self-promotion, providing users space to publish their work experience, education, specialties and interests. Groups can be joined (Cornell Alumni, ABI) and people can be “recommended.”
- **Facebook:** Social networking site, originally designed for college students. Pictures and videos can be uploaded, and depending upon “privacy” settings

[ 6 ]

## Definitions

### Twitter

- Micro blogging = combination instant messaging and blogging. Text-based posts of 140 characters or less, displayed on author's profile page and delivered to the author's subscribers, known as "followers."

[ 7 ]

## Definitions

### Snapchat

- A photo messaging application where users can take photos, record videos, add text and drawings, and send them to their friends. These sent photographs and videos are known as "Snaps." Users set a time limit for how long recipients can view their Snaps from 1 to 10 seconds after which they disappear (and deleted from Snapchat's servers).

[ 8 ]

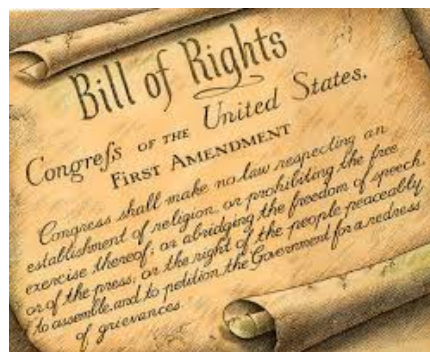
## Definitions

### Instagram

- an online mobile photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, and share them on a variety of social networking platforms, such as Facebook, Twitter, Tumblr and Flickr. Users can also apply digital filters to their images. The maximum duration for Instagram videos is 15 seconds.

[ 9 ]

## First Amendment Issues



- Social media is speech
- First Amendment prescribes the outer limit of attorney speech
- More protection for speaking about matters of public concern, less for commercial speech
- The government may prohibit commercial speech that is “false, deceptive or misleading”
- 1<sup>st</sup> Amendment sets boundaries of private liability for defamatory speech

[ 10 ]

## Old media rules apply when attorneys use new media



- Advertising on social media may be regulated
- When the speech on social media is about a matter of public concern, the speech is entitled to the greatest protection
- Speech that is defamatory is analyzed/treated whether it is broadcast on old or new media

[ 11 ]

## Common Ethics Perils When Attorneys Use Social Media



[ 12 ]

## DC Bar Ethics Opinion 370

The Rules apply to a number of different social media or social networking activities that an attorney or law firm may be engaged in, including:

1. Connecting and communicating with clients, former clients or other lawyers on social networking sites;
2. Writing about an attorney's own cases on social media sites, blogs or other internet-publishing based websites;
3. Commenting on or responding to online reviews or comments;
4. Self-identification by attorneys of their own "specialties," "skills" and "expertise" on social media sites;
5. Reviewing third-party endorsements received by attorneys on their personal or law firm pages; and,
6. Making endorsements of other attorneys on social networking sites.

( 13 )

## The Rules that are potentially implicated by social media include:

- Rule 1.1 (Competence)
- Rule 1.6 (Confidentiality of Information)
- Rule 1.7 (Conflict of Interest: General)
- Rule 1.18 (Duties to Prospective Client)
- Rule 3.3 (Candor to Tribunal)
- Rule 5.1 (Responsibilities of Partners, Managers, and Supervisory Lawyers)
- Rule 5.3 (Responsibilities Regarding Non-Lawyer Assistants)
- Rule 7.1 (Communications Concerning a Lawyer's Services)
- Rule 8.4 (Misconduct)
- Rule 8.5 (Disciplinary Authority; Choice of Law)

( 14 )



## Risks Inherent in the Use of Social Media

- ...Lawyers must be cognizant of the benefits and risks of the use of social media and their postings on social media sites. Social networking sites, and social media in general, make it easier to blur the distinctions between communications that are business and those that are personal.
- Communications via social media are inherently less formal than more traditional or established forms of communication.
- Lawyers and law firm employees must be reminded of the need to maintain confidentiality with regard to clients and client matters in all communications.
- It is recommended that all law firms have a policy in place regarding employees' use of social networks.
- Lawyers in law firms have an ethical duty to supervise subordinate lawyers and non-lawyer staff to ensure that their conduct complies with the applicable Rules, including the duty of confidentiality. *See Rules 5.1 and 5.3.*

{ 15 }

## The Requirement of Candor

- Content contained on a lawyer's social media pages must be truthful and not misleading.
- Statements on social media could expose an attorney to charges of dishonesty under Rule 8.4 or lack of candor under Rule 3.3, if the social media statements conflict with statements made to courts, clients or other third parties, including employers.
- Similarly, statements on social media could expose a lawyer to civil liability for defamation, libel or other torts.

{ 16 }

## The Formation of an Attorney-Client Relationships: Cautions

- It is permissible for lawyers to participate in online chat rooms and similar arrangements through which attorneys could engage in real time, or nearly real time communications with internet users.
- Lawyers must avoid the provision of specific legal advice in order to prevent the formation of an attorney-client relationship.
- Opinion 302 sets forth "best practices" guidance on internet communications, with the intent of avoiding the inadvertent formation of an attorney-client relationship. One of the suggested "best practices" included the use of a prominent disclaimer. *Id.*
- However, we have reiterated "that even the use of a disclaimer may not prevent the formation of an attorney-client relationship if the parties' subsequent conduct is inconsistent with the disclaimer." D.C. Ethics Op. 316.

[ 17 ]

## Rule 1.18: A duty of confidentiality with regard to a prospective client

- The guidance of Rule 1.18 is of particular importance in social networking, where lawyers may self-identify themselves as attorneys and where, most likely, those "connected" to the lawyer will be aware that the user is an attorney.
- The mere knowledge that a friend is an attorney does not give rise to a reasonable expectation that interactions with that attorney would create a prospective or actual client relationship, or its attendant duty of confidentiality.

[ 18 ]

## Attorneys may write about their own cases on social media sites, blogs or other internet-based publications, with the informed consent of their clients – Rule 1.6

- While lawyers may ethically write about their cases on social media, lawyers must take care not to disclose confidential or secret client information in social media posts
  - Because Rule 1.6 extends to even information that may be known to other people, the prudent lawyer will obtain client consent before sharing any information regarding a representation or disclosing the identity of a client.
  - Even if the attorney is reasonably sure that the information being disclosed would not be subject to Rule 1.6, it is prudent to obtain explicit informed client consent before making such posts.
  - With or without client consent, attorneys should exercise good judgment and great caution in determining the appropriateness of such posts. Consideration should be given to the identity of the client and the sensitivity of the subject matter, even if the client is not overtly identified. It is advisable that the attorney share a draft of the proposed post or blog entry with the client, so there can be no miscommunication regarding the nature of the content that the attorney wishes to make public. It is also advisable, should the client agree that the content may be made public, that the attorney obtain that client consent in a written form.

( 19 )

## Disclosures on social media must be compliant with Rule 7.1.

- Rule 7.1 governs all communications about a lawyer's services, including advertising. These Rules extend to online writings, whether on social media, a blog or other internet-based publication, regarding a lawyer's own cases. Such communications are subject to the Rules because they have the capacity to mislead by creating the unjustified expectation that similar results can be obtained for others. Care must be taken to avoid material misrepresentations of law or fact, or the omission of facts necessary to make the statement considered as a whole not materially misleading. Accordingly, social media posts regarding a lawyer's own cases should contain a prominent disclaimer making clear that past results are not a guarantee that similar results can be obtained for others.

( 20 )

## Specialization: Skills and Practice Areas

- Many social media sites, like LinkedIn, allow attorneys to identify skills and areas of practice.
- The District of Columbia does not prohibit statements regarding specialization or expertise. Accordingly, District of Columbia attorneys are ethically permitted to identify their skills, expertise and areas of practice, subject to Rule 7.1(a).

[ 21 ]

## Information about an Attorney Must be Accurate

- For websites or social media sites where the attorney does not have editorial control over content or the postings of others, we do not believe that the Rules impose an affirmative duty on a lawyer to monitor the content of the sites; however, under certain circumstances, it may be appropriate for the attorney to request that the poster remove the content, to request that the social networking site remove the content, or for the attorney to post a curative response addressing the inaccurate content.

[ 22 ]

## Pennsylvania Bar Association Formal Opinion 2014-300

{ 23 }

Provides a broad overview of ethical concerns raised by social media, including:

- 1. Whether attorneys may advise clients about the content of the clients' social networking websites, including removing or adding information.
- 2. Whether attorneys may connect with a client or former client on a social networking website.
- 3. Whether attorneys may contact a represented person through a social networking website.
- 4. Whether attorneys may contact an unrepresented person through a social networking website, or use a pretextual basis for viewing information on a social networking site that would otherwise be private/unavailable to the public.

{ 24 }

- 5. Whether attorneys may use information on a social networking website in client-related matters.
- 6. Whether a client who asks to write a review of an attorney, or who writes a review of an attorney, has caused the attorney to violate any Rule of Professional Conduct.
- 7. Whether attorneys may comment on or respond to reviews or endorsements.
- 8. Whether attorneys may endorse other attorneys on a social networking website.
- 9. Whether attorneys may review a juror's Internet presence.
- 10. Whether attorneys may connect with judges on social networking sites.

{ 25 }

**This Committee concludes that:**

- 1. Attorneys may advise clients about the content of their social networking websites, including the removal or addition of information.
- 2. Attorneys may connect with clients and former clients.
- 3. Attorneys may not contact a represented person through social networking websites.
- 4. Although attorneys may contact an unrepresented person through social networking websites, they may not use a pretextual basis for viewing otherwise private information on social networking websites.
- 5. Attorneys may use information on social networking websites in a dispute.

{ 26 }

6. Attorneys may accept client reviews but must monitor those reviews for accuracy.
7. Attorneys may generally comment or respond to reviews or endorsements, and may solicit such endorsements.
8. Attorneys may generally endorse other attorneys on social networking websites.
9. Attorneys may review a juror's Internet presence.
10. Attorneys may connect with judges on social networking websites provided the purpose is not to influence the judge in carrying out his or her official duties.

{ 27 }

## Tips for Using Social Media

- Decide why you are using social media
- Develop a theme and a tone
- Be wary of “advertising” yourself or your firm
- Report facts objectively and offer opinions, but be clear in distinguishing between the two
- Moderate comments on your blog – beware of spam!

{ 28 }

## Why lawyers get in trouble with social media



[ 29 ]

## How can I use social media?

- Determine the purpose of the communication;
- Determine ethical constraints on such a communication; and
- Determine whether social media constitutes a reasonable approach to delivering the message within established ethical bounds.

[ 30 ]



## Social Media and Advertising Law

- FTC Act Section 5: “Unfair or Deceptive Acts or Practices in or Affecting Commerce are Hereby Declared Unlawful.”
- **Four Core Principles**
  - Advertising must be truthful and not misleading;
  - Advertising must substantiate any express or implied claims;
  - Advertising cannot be unfair or deceptive; and
  - Any disclosures necessary to make an ad accurate must be clear and conspicuous.
- State UDAPs may be broader and have private right of action.
- Ethics rules regarding attorney advertising.
- Advertising and promotion in SM are subject to the same federal and state regulations as traditional media.

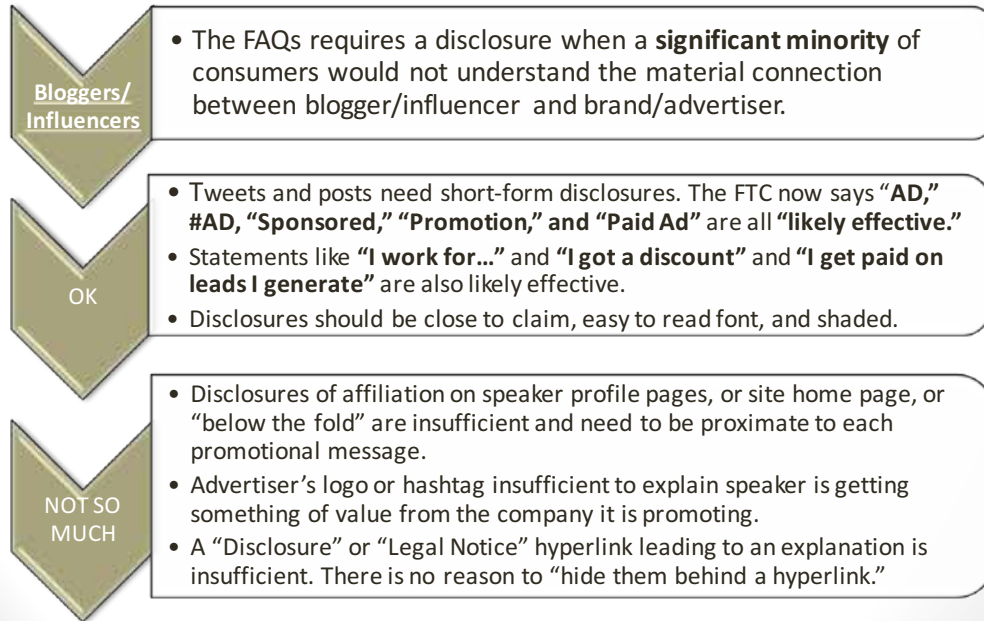
{ 31 }

### FTC Revised Endorsement and Testimonial Guidelines (2009)

- Guidelines address application of Section 5 to the use of endorsements and testimonials in advertising.
- Advertisers are subject to liability for false or unsubstantiated statements made through endorsements or for failure to disclose material connection between themselves and endorsers.
- Revised guidelines require disclosure in any blogs, SM, and UGC of speaker’s “material connection” to an advertiser.

{ 32 }

## What is an effective disclosure? What works what does not?



{ 33 }

## Best practices:

- Social media guidelines / policy;
- Advise employees to disclose the material connection;
- Beware of EEOC limits;
- Monitor brand mentions;
- Incorporate guidelines into PR/Ad agency contracts; and
- Take corrective action.

{ 34 }

# Social Media Content IP Liability Issues

- Key questions - What is the content? What is the intended use? Do you need permission? Does the use fall within the scope of permission?
- Review all third party copyrightable material and trademark usage.
- Nature of Third Party Platform usage (API, reposting)
- State publicity rights protect individual's image, name, and likeness from commercial exploitation
- Lanham Act false advertising (competitors) or false endorsement (others) claims
- Commercial v. non-commercial speech

**Key takeaway:**

Understand where 3rd party content comes from, if you're allowed to use it, how it will be used and what the rules of use are.

35

# Torn from the headlines: Data Security / Breach

**Bloomberg Businessweek**  
Companies & Industries

**As Data Breach Woes Continue, Target's CEO Resigns**

By Michael May and Dawn Laviecki | May 01, 2014

Target CEO Greg Steinhilber talks to Black Friday book buyers on Nov. 27, 2013, in Minneapolis. (AP)

Target's chairman and chief executive officer, Greg Steinhilber, a 35-year company veteran, is stepping down, as the massive pre-Christmas data breach suffered by the Minnesota retailer continues to rattle the company. The decision is effective immediately, according to a statement posted today on the company's website. John Mulligan, Target's chief financial officer, has been appointed as interim president.

**THE WALL STREET JOURNAL** | TECH

**WORLD CUP 2014**

**Corporate Boards Race to Shore Up Cybersecurity**  
Downside Grapple With Issues Once Consigned to Tech Experts

By GARY YARON

Ellen Rhee, Visa's chief legal officer, with more data encrypted (Bloomberg News)

After a series of high-profile data breaches and warnings, corporate boards are waking to cybersecurity, grappling with security issues they once relegated to technology experts.

Computer hacking is on the agenda these days when **Yahoo! Co.** (YHOO) is

36

## Legal and Ethical Duty

- To Protect
  - WISP and program
  - HIPAA? Credit Cards? HR (SS#s)
  - Train
  - Assess and remediate
- To Notify
  - Breach response plan and program



From NIST SP 800-61

{ 37 }

## Where are the threats?

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>• Inside threats           <ul style="list-style-type: none"> <li>– Employee negligence               <ul style="list-style-type: none"> <li>• Security failures</li> <li>• Lost mobile devices</li> </ul> </li> <li>– Employee ignorance               <ul style="list-style-type: none"> <li>• Improper disposal of personal information (dumpsters)</li> <li>• Lack of education and awareness</li> </ul> </li> <li>– Malicious employees</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Outside threats           <ul style="list-style-type: none"> <li>– Hackers               <ul style="list-style-type: none"> <li>• Malware</li> <li>• Ransomware</li> <li>• Phishing and Spear Phishing</li> </ul> </li> <li>– Thieves (including Social Engineering Tools)</li> <li>– Vendors</li> </ul> </li> </ul> |
|--|---|

{ 38 }

## Become “Compromise” Ready

- Security safeguards and assessments
  - Understand where assets and sensitive data are located and protect
  - Ensure ongoing “Reasonable security”
  - Employ detection capabilities
- Invest in appropriate technology and personnel
- Prepare for incidents
- Ongoing diligence

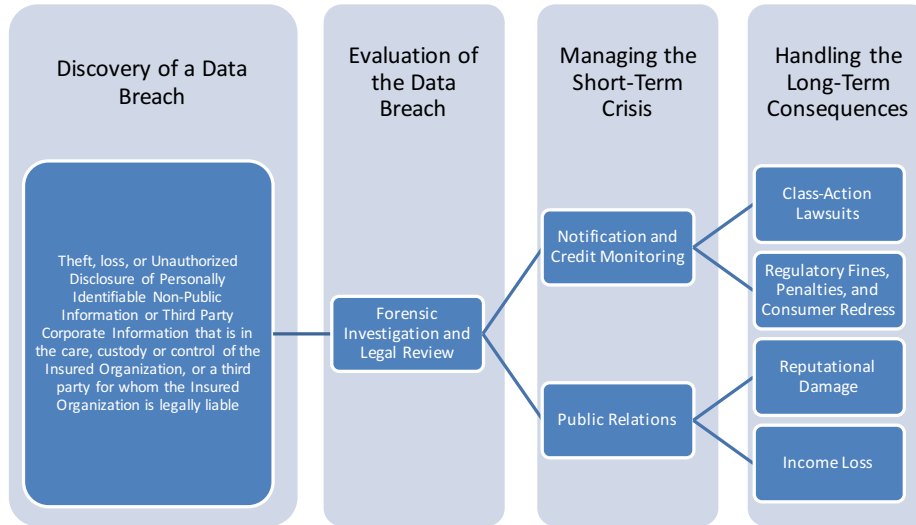
{ 39 }

## Program Elements:

- Establishing Plan, Setting Goals and Measuring Performance
- Document Retention/Destruction Schedule and Litigation Hold Processes
- Assessments and Remediation
- Training
- Tabletop Exercises with Response Team
- Cyber Insurance
- Vendor Management

{ 40 }

## What Should Happen If There Is a Suspected Security Incident or Breach, and When and How?



{ 41 }

## Costs of Response

- Forensics
- Notification costs
- Credit monitoring
- Call center
- Crisis response
- Legal fees
- Potential fines / damages
- Defense costs/settlement expenses
- Reputational injury

CATEGORY	DESCRIPTION	COSTS
1). Notification Costs	<ul style="list-style-type: none"> <li>• Address list management</li> <li>• Printing, Inserting, Mailing</li> <li>• Post-Mailing Call Services</li> <li>• Returned Mail</li> </ul>	\$2,308,350
2). Credit Monitoring	<ul style="list-style-type: none"> <li>• Flat Fee —\$4</li> <li>• Redemption — \$15 @15% redemption rate</li> </ul>	AVG: \$5,512,500

{ 42 }

## Ten Rules for Lawyers Using Social Media

1. Social Media Profiles and Posts May Constitute Legal Advertising.
2. Avoid Making False or Misleading Statements.
3. Avoid Making Prohibited Solicitations.
4. Do Not Disclose Privileged or Confidential Information.
5. Do Not Assume You Can “Friend” Judges.

{ 43 }

## Ten Rules for Lawyers Using Social Media

6. Avoid Communications With Represented Parties.
7. Be Cautious When Communicating With Unrepresented Third Parties.
8. Beware of Inadvertently Creating Attorney-Client Relationships.
9. Beware of Potential Unauthorized Practice Violations.
10. Tread Cautiously with Testimonials, Endorsements, and Ratings.

{ 44 }

**Social Media and the Law — False Advertising,  
SPAM and Privacy and Data Security Issues**

Alan L. Friel  
Baker & Hostetler LLP  
afriel@bakerlaw.com

**I. Overview**

A. Legal Landscape

1. General
2. FTC Endorsement Guides and Native Ad Guidance
3. Privacy and Data Security
4. SPAM

B. Practical Guidance

**II. Analysis of Legal Landscape**

A. General

1. *US. Law:* Section 5 of FTC Act and state equivalents, as well as specific statutes and regulations governing emerging technology and communications). Also, labor laws as relate to employee speech.
2. *Contract:* Terms of Use; EULAs
3. *Industry Self-regulation and Guidelines:* WOMMA ([www.WOMMA.org](http://www.WOMMA.org): Honesty and transparency); Cross-industry Self-Regulatory Program for OBA (NAI, IAB, BBB, 4As, AAF & ANA = Digital Advertising Alliance (DAA)) - [www.AboutAds.info](http://www.AboutAds.info)); [IAB Native Advertising Playbook](#).

B. FTC Endorsement Guides (16 C.F.R. Part 255) [[http://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr255\\_main\\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr255_main_02.tpl)] or <https://www.ftc.gov/sites/default/files/documents/one-stops/advertisement-endorsements/091005revisedendorsementguides.pdf>]

1. FTC Endorsement Guides require *disclosure of*



## 2017 WINTER LEADERSHIP CONFERENCE

- a. a connection
  - b. between a seller and an endorser
  - c. that might materially affect
  - d. the weight or credibility of the endorsement
2. An *endorsement* is any:
- a. advertising message that
  - b. consumers believe
  - c. represents the opinions, beliefs, experience, etc. of a person other than the sponsoring advertiser, such as:
    - (1) Restaurant or Product Reviewers
    - (2) Bloggers
    - (3) Celebrities online and talk shows
3. A *material connection* is one that matters to the consumer - that might affect his or her choice
4. In other words, one that isn't reasonably expected, such as:
- a. Seller is compensating endorser (including product and benefits)
  - b. Endorser is employee or business associate of seller
  - c. Endorser is related to seller
5. Disclosure should be part of the message - *clear, conspicuous and proximate*
6. For example:
- a. Acme Co. provided this product for me to review
  - b. XYZ Co. sent me to Adventureland to experience their theme park
7. Short form, icons and mini urls:
- a. FTC Dot Com Disclosure Rules  
[\[https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf\]](https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf)

- b. On Twitter: #paid, #ad or "Sponsored"
- c. CMP.LY Service: "Sponsored: <http://cmp.ly/2>" - links to:  
"I have a material connection because I received a gift or sample of a product for consideration in preparing to write this content. I was/am not expected to return this item or gift after my review period."

8. Enforcement

- a. Early 2010 Ann Taylor Gifts to Bloggers; FTC Closure Letter [<https://www.ftc.gov/enforcement/cases-proceedings/closing-letters/anntaylor-stores-corporation>]
- b. Fall 2010 FTC Complaint against Reverb Communications and Consent Order [<http://www.ftc.gov/os/caselist/0923199/index.shtm>]
  - (1) PR firm hired to promote video games
  - (2) Firm's employees allegedly poses as iTunes customers
  - (3) Posted reviews of client video games
  - (4) Did not disclose the connection
- c. March 2011 FTC Legacy Learning Complaint and Settlement Order [<http://www.ftc.gov/os/caselist/1023055/index.shtm>]
  - (1) "Ad review affiliates"
  - (2) Failure to disclose
  - (3) \$250,000
- d. May 2011 FTC Complaint and Consent Order with an individual consumer (Marsha Kellogg) for making misrepresentations in an endorsement (that she made more money using a certain program than she had, in fact, made): FTC and State of Colorado v. Russell Dalbey, et al. [<https://www.ftc.gov/enforcement/cases-proceedings/092-3062/dalbey-russell-t-et-al>]
- e. November 16, 2011 FTC Closing Letter to Hyundai: No action since blogger' s failure to disclose payments violated company's social media policy and company took corrective action upon discovery of violations.

- f. March 20, 2014 FTC Closing Letter to Cole Hahn: Providing an entry to a contest or sweepstakes by posting on social media is an endorsement that requires disclosure the person may be motivated by a chance to win. #ColeHahnSweepstakes is okay, but #WonderingSole or #Sweeps is not.
  - g. International: UK Office of Fair Trading July 2010 investigation under the Enterprise Act of 2002 and 2008 Consumer Protection from Unfair Trading Regulation regarding Handpicked Media's engagement of bloggers for hire without disclosure to consumers that posts were paid for.
  - h. What not to do: 5/6/11 Allure Beauty to Bloggers:  
  
"...we send new and interesting products to a select group of bloggers ...we ask you to follow our Mother's philosophy that 'if you can't say anything nice, don't say anything at all.'"
9. Competitor Claims -Kim Kardashian Diet Tweeting Case
10. December 2015 FTC Guidance on Native Advertising: Gives examples of what is and is not sufficient disclosure of a material connection and what is commercial rather than editorial.
- C. FTC Guidance: Native Advertising
- 1. A Guide for Business: <https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses>
  - 2. Enforcement Policy Statement on Deceptively Formatted Advertisements: [https://www.ftc.gov/system/files/documents/public\\_statements/896923/151222deceptiveenforcement.pdf](https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf)
- D. Cross-Device Tracking
- 1. FTC Staff Report: [https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc\\_cross-device\\_tracking\\_report\\_1-23-17.pdf](https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf)
    - a. Concurring Statement of Commissioner Maureen Ohlaussen: [https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/cross-device\\_tracking\\_report\\_concurring\\_statement\\_of\\_commissioner\\_ohlhausen\\_1-23-17.pdf](https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/cross-device_tracking_report_concurring_statement_of_commissioner_ohlhausen_1-23-17.pdf)

- E. FTC Endorsement Guides FAQs
1. FTC's Endorsement Guides: What People Are Asking:  
[https://www.ftc.gov/system/files/documents/plain-language/pdf-0205-endorsement-guides-faqs\\_0.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0205-endorsement-guides-faqs_0.pdf)
  2. Recent Consent Decrees
    - a. FTC v. Mercola.com, LLC (2016)
      - (1) Complaint:  
<https://www.ftc.gov/system/files/documents/cases/160414/mercolacmpt.pdf>
      - (2) Complaint Exhibits:  
<https://www.ftc.gov/system/files/documents/cases/160414/mercolaexhibitsa-h.pdf>
      - (3) Stipulation for Entry of Permanent Injunction and Other Equitable Relief:  
<https://www.ftc.gov/system/files/documents/cases/160414/mercolastip.pdf>
      - (4) Press Release: <https://www.ftc.gov/news-events/press-releases/2017/02/ftc-providing-full-refunds-mercola-brand-tanning-system>
    - b. FTC v. Aura Labs, Inc. (2016)
      - (1) Complaint:  
[https://www.ftc.gov/system/files/documents/cases/161212/aura\\_labs\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/161212/aura_labs_complaint.pdf)
      - (2) Order:  
[https://www.ftc.gov/system/files/documents/cases/161212/aura\\_labs\\_final\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/161212/aura_labs_final_order.pdf)
    - c. In the Matter of Warner Bros. Home Entertainment, Inc. (2016)
      - (1) Complaint:  
[https://www.ftc.gov/system/files/documents/cases/161811/warner\\_bros\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/161811/warner_bros_complaint.pdf)
      - (2) Complaint Exhibits:  
[https://www.ftc.gov/system/files/documents/cases/161811/warner\\_bros\\_complaint\\_exhibits.pdf](https://www.ftc.gov/system/files/documents/cases/161811/warner_bros_complaint_exhibits.pdf)

- (3) Decision and Order:  
[https://www.ftc.gov/system/files/documents/cases/161811c-4595\\_warner\\_bros\\_do.pdf](https://www.ftc.gov/system/files/documents/cases/161811c-4595_warner_bros_do.pdf)
  - (4) Letters to Commenters:  
[https://www.ftc.gov/system/files/documents/cases/letters\\_to\\_commenters.pdf](https://www.ftc.gov/system/files/documents/cases/letters_to_commenters.pdf)
- F. UGC, Rights of Publicity and Social Media Promotions:
1. UGC may infringe third party rights. DMCA and CDA may provide partial protection if campaigns are carefully crafted.
  2. Courts split on whether CDA immunity applies to rights of publicity claims. Compare *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir. 2007) with *Doe v. Friendfinder Network, Inc.* 540 F.Supp2d 288 (D.N.H, 2008).
  3. Facebook "Like" program is subject to multiple class actions. On December 16, 2011 a federal district court rejected a motion to dismiss finding: 1) Facebook did not qualify for CDA immunity since it created the sponsored ads; 2) non-celebrity users are economically harmed when their rights of publicity are violated; and 3) issues of fact existed as to if users knowingly consented to association of themselves to the advertisers they "liked" via "sponsored ads" to the users' friends. *Fraley et al. v. Facebook, Inc.*, 2011 U.S. Dist Lexis 145195 (Case No. 11-CV-01726-LHK).
- G. Privacy and Data Security
1. FTC staff 2010 Online Privacy Report December 1, 2010, "*Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers*" [<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>] made final on March 26, 2011 as a commission report, a copy of which is at [http://https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf](https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf)
    - a. Privacy by Design;
    - b. Self-regulation by industry; and
    - c. Federal legislation to set baseline privacy requirements, data security requirements and special requirements for data brokers.

2. White House March 2012: "*Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy*"  
[\[http://www.whitehouse.gov/sites/default/files/privacy-final.pdf\]](http://www.whitehouse.gov/sites/default/files/privacy-final.pdf), which calls for:
  - a. Privacy Bill of Rights;
  - b. Simplification of consumer choice and greater transparency; and
  - c. Calls for industry self-regulation and new legislation.
3. FTC "Do Not Track" Proposal (400 + comments):  
[\[http://www.ftc.gov/opa/2010/12/privacyreport.shtm\]](http://www.ftc.gov/opa/2010/12/privacyreport.shtm)
4. FTC and Data Security Overview and 1016 Year in Review:  
[\[https://www.ftc.gov/reports/privacy-data-security-update-2016\]](https://www.ftc.gov/reports/privacy-data-security-update-2016)
5. Location-aware privacy issues
  - a. Recent issues / lawsuits re iPhone/Android tracking
  - b. Mobile Apps: Platform and Carrier Rules
  - c. California AG applies piracy policy requirement to mobile apps  
[\[http://ag.ca.gov/cms\\_attachments/press/pdfs/n2630\\_updated\\_mobile\\_apps\\_info.pdf\]](http://ag.ca.gov/cms_attachments/press/pdfs/n2630_updated_mobile_apps_info.pdf)
6. Online Behavioral Advertising (OBA) issues
  - a. Class action law suits
  - b. Typically allege: ( 1) invasion of privacy; (2) violation of the Electronic Communications Privacy Act (18 U.S.C. Section 2510 et seq); (3) violations of the Computer Fraud and Abuse Act (18 U.S.C. Section 1030 et seq); (4) trespass to chattel; and (5) unfair business practices.
7. Flash Cookies, HTML5 and ETag Respawning Cases Many pending. Several knocked out for lack of harm / injury.
8. Children's Privacy
  - a. COPPA (15 U.S.C. Section 6501 et seq)
  - b. FTC 2011 Playdom Complaint and Consent Order  
<http://www.ftc.gov/os/caselist/1023036/index.shtm>  
-- \$3 Million

9. December 16, 2010 Department of Commerce Internet Policy Task Force privacy green paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."  
[\[https://www.ntia.doc.gov/files/ntia/publications/iptf\\_privacy\\_greenpaper\\_12162010.pdf\]](https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf)
  10. Recent Developments in the EU: EU Safe Harbor ruled inadequate in late 2015. New arrangement between U.S. Commerce Department and EU Data Protection Authorities now in place:  
<https://www.commerce.gov/page/eu-us-privacy-shield>. New EU data protection scheme, the General Data Protection Regulation, replaces current Data Protection Directive, in May 2018:  
[http://europa.eu/rapid/press-release\\_MEMO-15-6385\\_en.htm](http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm) and  
<http://www.eugdpr.org/>
- H. TCPA (47 U.S.C. Section 227 et seq.) / CAN-SPAM (15 U.S.C. Sections 7701-7713)
1. Overview - opt-in scheme for mobile; opt-out for e-mail
  2. 2015 FCC Order refines regulations and provides guidance, including technical requirements for promotional text opt-in (express written consent): <https://www.fcc.gov/document/tpa-omnibus-declaratory-ruling-and-order>

### III. Practical Guidance

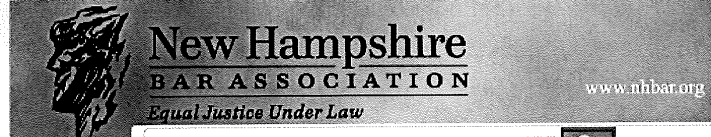
- A. Social Media Policies
1. For employees engaged in marketing
  2. For other employees
  3. Limits on employer restrictions of employee speech -recent NLRB settlement with CT ambulance company/complaints against Reuters
  4. Restrictions on use of company email
  5. Responding to tweets/other social media posts about company
  6. Beware chilling employee free speech or right to organize or comment on employment conditions (See NLRB guidance)
- B. Beware UGC programs and Rights of Publicity issues
- C. Updates to Privacy Policy

1. Obtain consent before treating data differently than promised when it was gathered.
  2. FTC Gateway Decision  
[<https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917do0423047.pdf>]
- D. Vendor Contracts
1. Due Diligence
  2. Negotiation
  3. Data Security
  4. Indemnification
  5. Other Key Terms
- E. FTC Endorsement Guides [http://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr255\\_main\\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?SID=e37d3cd088c6b4724a389338f9c3e141&mc=true&tpl=/ecfrbrowse/Title16/16cfr255_main_02.tpl) or  
<http://ftc.gov/os/2009/10/091005revisedendorsementguides.pdf>
1. To limit potential liability
    - a. Advertiser should ensure its endorsers receive guidance/training re need to ensure statements are truthful/substantiated
    - b. Advertiser should monitor sponsored bloggers, etc. and take steps to halt continued publication of deceptive claims when discovered
    - c. Employee relationship must be disclosed and employees trained and monitored



## RESOURCES

- *FTC Issues Native Ad Guidance* (December 2015) By Alan L. Friel, Fernando A. Bohorquez, Jr. and Alan M. Pate, BakerHostetler IP Intelligence Report – [http://www.ipintelligencereport.com/2015/12/30/ftc-issues-native-ad-guidance/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+IPIntelligence+%28IP+Intelligence+Report%29](http://www.ipintelligencereport.com/2015/12/30/ftc-issues-native-ad-guidance/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IPIntelligence+%28IP+Intelligence+Report%29)
- *Data Protection Issues Corporation Counsel Should Understand* (August 2015) By Alan L. Friel, Financier Worldwide Magazine – <http://www.financierworldwide.com/data-protection-issues-corporate-counsel-should-understand/>
- *FTC Clarifies Native and Online Ad Obligations* (June 17, 2015) By Alan L. Friel and Fernando A. Bohorquez, Jr., BakerHostetler Data Privacy Monitor – <http://www.dataprivacymonitor.com/social-media/ftc-clarifies-native-and-online-ad-obligations>
- *To Avoid Claims, Assess Privacy Impacts of Marketing and CRM* (April 2015) By Alan L. Friel, Law Journal Newsletters - e-Commerce Law & Strategy – [http://www.lawjournalnewsletters.com/issues/ljn\\_ecommerce/31\\_12/news/to\\_avoid\\_claims\\_assess\\_privacy\\_impacts\\_of\\_marketing\\_and\\_crm-161021-1.html](http://www.lawjournalnewsletters.com/issues/ljn_ecommerce/31_12/news/to_avoid_claims_assess_privacy_impacts_of_marketing_and_crm-161021-1.html) or <http://www.dataprivacymonitor.com/cybersecurity/to-avoid-claims-assess-privacy-impacts-of-marketing-and-crm/>
- *Navigating the Legal Risks of Native Advertising* (March 5, 2015) By Alan L. Friel, Law360 – <http://www.law360.com/articles/627657>
- *Navigating FTC's Guidance on Social Marketing* (Nov 30, 2009) By Alan L. Friel, AdWeek – <http://www.adweek.com/news/advertising-branding/navigating-ftcs-guidance-social-media-marketing-100969>
- *Employers Need to Review and Revise Social Media, Blogging and Privacy Policies after NLRB General Counsel Report* (June 5, 2012) By Alan L. Friel, Barry J. Bendes and David C. Kurtz, www.martindale.com – [http://www.martindale.com/labor-employment-law/article\\_Edwards-Wildman-Palmer-LLP\\_1524040.htm](http://www.martindale.com/labor-employment-law/article_Edwards-Wildman-Palmer-LLP_1524040.htm)
- *Growing Promotional Use of Social Media in the Government's Crosshairs -- the New FTC Guidelines* (Winter 2009/2010) By Alan L. Friel, ME/Insights (The Association of Media and Entertainment Counsel) – <http://www.dataprivacymonitor.com/wp-content/uploads/sites/188/2015/06/Friel-Article-2010.pdf>
- *Safeguarding Brand Reputation in Social Media* (June 19, 2013) By Alan L. Friel, Akash Sachdeva, Jesse Brody and Jatinder Bahra, The Daily Report (ALM) – <http://media.lockelord.com/files/upload/Top%20Ten%20Issues%20for%20Companies%20Regarding%20Social%20Media.pdf>



**New Hampshire**  
BAR ASSOCIATION  
*Equal Justice Under Law*

www.nhbar.org

Home

Go

Need a Lawyer? | Law-Related Education | NHBA CLE | NHBA Insurance Agency

About the Bar  
For Members  
For the Public  
Legal Links  
Publications  
Newsroom  
Online Store  
Vendor Directory  
NH BAR FOUNDATION  
Judicial Branch  
NHMCLE SC RULE 53

**MyNHBar**  
Member Login  
Member Portal  
Casemaker

**Ethics Committee Advisory Opinion #2012-13/05**  
**Social Media Contact with Witnesses in the Course of Litigation**

By the NHBA Ethics Committee

*This opinion was submitted for publication by the NHBA Board of Governors at its June 20, 2013 meeting.*

**RULE REFERENCES:**

- 1.1(b) and (c) Competence
- 1.3 Diligence
- 3.4 Fairness to opposing party and counsel
- 4.1(a) Truthfulness in statements to others
- 4.2 Communications with others represented by counsel
- 4.3 Dealing with the unrepresented person
- 4.4 Respect for the rights of third persons
- 5.3 Non-lawyer assistants
- 8.4(a) Unethical conduct through an agent

**SUBJECTS:**

- Competence and Diligence
- Truthfulness
- Fairness to Opposing Parties, Counsel, and Third Parties
- Contact with Witnesses
- Agents of Lawyers; Acting Through Others

**ANNOTATION**

The Rules of Professional Conduct do not forbid use of social media to investigate a non-party witness. However, the lawyer must follow the same rules which would apply in other contexts, including the rules which impose duties of truthfulness, fairness, and respect for the rights of third parties. The lawyer must take care to understand both the value and the risk of using social media sites, as their ease of access on the internet is accompanied by a risk of unintended or misleading communications with the witness. The Committee notes a split of authority on the issue of whether a lawyer may send a social media request which discloses the lawyer's name - but not the lawyer's identity and role in pending litigation - to a witness who might not recognize the name and who might otherwise deny the request.<sup>1</sup> The Committee finds that such a request is improper because it omits material information. The likely purpose is to deceive the witness into accepting the request and providing information which the witness would not provide if the full identity and role of the lawyer were known.

**QUESTION PRESENTED**

What measures may a lawyer take to investigate a witness through the witness's social media accounts, such as Facebook or Twitter, regarding a matter which is, or is likely to be, in litigation?

**FACTS**

The lawyer discovers that a witness for the opposing party in the client's upcoming trial has Facebook and Twitter accounts. Based on the information provided, the lawyer believes that statements and information available from the witness's Facebook and Twitter accounts may be relevant to the case and helpful to the client's position. Some information is available from the witness's social media pages through a simple web search. Further information is available to anyone who has a Facebook account or who signs up to follow the witness on Twitter. Additional information is available by "friending" the witness on Facebook or by making a request to follow the witness's restricted Twitter account. In both of those latter instances, the information is only accessible after the witness has granted a request.

**ANALYSIS**

*General Principles*

The New Hampshire Rules of Professional Conduct do not explicitly address the use of social media such as Facebook and Twitter. Nonetheless, the rules offer clear guidance in most situations where a lawyer might use social media to learn information about a witness, to gather evidence, or to have contact with the witness. The guiding principles for such efforts by counsel are the same as for any other investigation of or contact with a

Depression...Alcoholism...  
Addiction...Personal or  
Professional Crises...

Support for  
NH Attorneys,  
Judges, Law  
Students

Meet the great  
people who make  
the difference

Outreach  
& Education

Strictly  
Confidential

NH Lawyers Assistance  
can help you put the  
pieces back together.  
877-224-6060

**LAWPAY**

Win more clients and  
build lifelong loyalty.

GET OUR NEW E-BOOK

witness.

First and foremost, the lawyer has a duty under Rules 1.1 and 1.3 to represent the client competently and diligently. This duty specifically includes the duties to:

- "Gather sufficient facts" about the client's case from "relevant sources," Rule 1.1(c)(1);
- Take steps to ensure "proper preparation," Rule 1.1(b)(4); and
- Acquire the skills and knowledge needed to represent the client competently. Rule 1.1(b)(1) and (b)(2).

In the case of criminal defense counsel, these obligations, including the obligation to investigate, may have a constitutional as well as an ethical dimension.<sup>2</sup> In light of these obligations, counsel has a general duty to be aware of social media as a source of potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation.

The duties of competence and diligence are limited, however, by the further duties of truthfulness and fairness when dealing with others. Under Rule 4.1, a lawyer may not "make a false statement of material fact" to the witness. Notably, the ABA Comment to this rule states that "[m]isrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements." Similarly, under Rule 8.4, it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Also, if the witness is represented by counsel, then under Rule 4.3, a lawyer "shall not communicate" with the witness "about the subject of the representation" unless the witness's lawyer has consented or the communication is permitted by a court order or law. Finally, under Rule 4.4, the lawyer shall not take any action, including conducting an investigation, if it is "obvious that the action has the primary purpose to embarrass, delay, or burden a third person."

The lawyer may not avoid these limitations by conducting the investigation through a third person. With respect to investigators and other non-lawyer assistants, the lawyer must "make reasonable efforts to ensure" that the non-lawyer's conduct "is compatible with the professional obligations of the lawyer." Rule 5.3(b). A lawyer may be responsible for a violation of the rules by a non-lawyer assistant where the lawyer has knowledge of the conduct, ratifies the conduct, or has supervisory authority over the person at a time when the conduct could be avoided or mitigated. Rule 5.3(c). Nor should a lawyer counsel a client to engage in fraudulent or criminal conduct. Rule 1.2(d). Finally, of course, a lawyer is barred from violating the rules through another or knowingly inducing the other to violate the rules. Rule 8.4(a).

#### ***Application of the General Principles to the Use of Social Media When Investigating a Witness***

*Is it a violation of the rules for the lawyer to personally view a witness's unrestricted Facebook page or Twitter feed?* In the view of the Committee, simply viewing a Facebook user's page or "following" a Twitter user is not a "communication" with that person, as contemplated by Rules 4.2 and 4.3, if the pages and accounts are viewable or otherwise open to all members of the same social media site. Although the lawyer-user may be required to join the same social media group as the witness, unrestricted Facebook pages and Twitter feeds are public for all practical purposes. Almost any person may join either Facebook or Twitter for free, subject to the terms-of-use agreement. Furthermore, membership is more common than not, with Facebook reporting that it topped one billion accounts in 2012.<sup>4</sup>

Other state bars' ethics committees are in agreement that merely viewing an unrestricted Facebook or Twitter account is permissible.<sup>2</sup> If, however, a lawyer asks the witness's permission to access the witness's restricted social media information, the request must not only correctly identify the lawyer, but also inform the witness of the lawyer's involvement in the disputed or litigated matter. At least two bar associations have adopted the position that sending a Facebook friend request in-name-only constitutes a misrepresentation by omission, given that the witness might not immediately associate the lawyer's name with his or her purpose and that, were the witness to make that association, the witness would in all likelihood deny the request.<sup>5</sup> (This point is discussed in more detail below.)

*May the lawyer send a Facebook friend request to the witness or a request to follow a restricted Twitter account, using a false name?* The answer here is no. The lawyer may not make a false statement of material fact to a third person. Rule 4.1. Material facts include the lawyer's identity and purpose in contacting the witness. For the same reason, the lawyer may not log into someone else's account and pretend to be that person when communicating with the witness.

*May the lawyer's client send a Facebook friend request or request to follow a restricted Twitter feed, and then reveal the information learned to the lawyer?* The answer depends on the extent to which the lawyer directs the client who is sending the request. Rule 8.4(a) prohibits a lawyer from accomplishing through another that which would be otherwise barred. Also, while Rule 5.3 is directed at legal assistants rather than clients, to the extent that the client is acting as a non-lawyer assistant to his or her own lawyer, Rule 5.3 requires the lawyer to advise the client to avoid conduct on the lawyer's behalf which would be a violation of the rules.

Subject to these limitations, however, if the client has a Facebook or Twitter account that reasonably reveals the client's identity to the witness, and the witness accepts the friend request or request to follow a restricted Twitter feed, no rule prohibits the client from sharing with the lawyer information gained by that means. In the non-social media context, the American Bar Association has stated that such contact is permitted in similar limitations. See ABA Ethics Opinion 11-461.<sup>4</sup>

*May the lawyer's investigator or other non-lawyer agent send a friend request or request to follow a restricted Twitter feed as a means of gathering information about the witness?* The non-lawyer assistant is subject to the

same restrictions as the lawyer. The lawyer has a duty to make sure the assistant is informed about these restrictions and to take reasonable steps to ensure that the assistant acts in accordance with the restrictions. Thus, if the non-lawyer assistant identifies him- or herself, the lawyer, the client, and the cause in litigation, then the non-lawyer assistant may properly send a social media request to an unrepresented witness.

The witness's own predisposition to accept requests has no bearing on the lawyer's ethical obligations. The Committee agrees with the Philadelphia Bar Association's reasoning: "The fact that access to the pages may readily be obtained by others who either are or are not deceiving the witness, and that the witness is perhaps insufficiently wary of deceit by unknown internet users, does not mean that deception at the direction of the inquirer is ethical." Phil. Bar Assoc., Prof. Guidance Comm., Op. 2009-02.

*May the lawyer send a request to the witness to access restricted information, using the lawyer's name and disclosing the lawyer's role?* The answer depends on whether the witness is represented. If the witness is represented by a lawyer with regard to the same matter in which the lawyer represents the client, the lawyer may not communicate with the witness except as provided in Rule 4.2. If the witness is not represented, the lawyer may send a request to access the witness's restricted social media profile so long as the request identifies the lawyer by name as a lawyer and also identifies the client and the matter in litigation. This information serves to correct any reasonable misimpression the witness might have regarding the role of the lawyer.

*May the lawyer send a request to the witness to access restricted information, when the request uses only the lawyer's name or the name of an agent, and when there is a reasonable possibility that the witness may not recognize the name and may not realize the communication is from counsel involved in litigation?* There is a split of authority on this issue, but the Committee concludes that such conduct violates the New Hampshire Rules of Professional Conduct. The lawyer may not omit identifying information from a request to access a witness's restricted social media information because doing so may mislead the witness. If a lawyer sends a social media request in-name-only with knowledge that the witness may not recognize the name, the lawyer has engaged in deceitful conduct in violation of Rule 8.4(c). The Committee further concludes omitting from the request information about the lawyer's involvement in the disputed or litigated matter creates an implication that the person making the request is disinterested. Such an implication is a false statement of material fact in violation of Rule 4.1. As noted above, the ABA Comment to this rule states that "[m]isrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements."

Deceit is improper, whether it is accomplished by providing information or by deliberately withholding it. Thus, a lawyer violates the rules when, in an effort to conceal the lawyer's identity and/or role in the matter, the lawyer requests access to a witness's restricted social media profile in-name-only or through an undisclosed agent. The Committee recognizes the counter-argument that a request in-name-only is not overtly deceptive since it uses the lawyer's or agent's real name and since counsel is not making an explicitly false statement. Nonetheless, the Committee disagrees with this counter-argument. By omitting important information, the lawyer hopes to deceive the witness. In fact, the motivation of the request in-name-only is the lawyer's expectation that the witness will not realize who is making the request and will therefore be more likely to accept the request. The New Hampshire Supreme Court has stated that honesty is the most important guiding principle of the bar in this state and that deceitful conduct by lawyers will not be tolerated. See generally, *RSA311:6; Feld's Case*, 149 N.H. 19, 24 (2002); *Kalil's Case*, 146 N.H. 466, 468 (2001); *Nardi's Case*, 142 N.H. 602, 606 (1998). The Committee is guided by those principles here.

The Committee notes that there is a conflict of authority on this issue. For example, the Committee on Professional Ethics for the Bar Association of New York City has stated:

We conclude that an attorney or her agent may use her real name and profile to send a "friend request" to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request. While there are ethical boundaries to such "friending," in our view they are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements. [Footnote omitted.]

NY City Bar, Ethic Op. 2010-2. Alternatively, the Philadelphia Bar Association concludes that such conduct would be deceptive. Phil. Bar Assoc., Prof. Guidance Comm., Op. 2009-02. That opinion finds that a social media request in-name-only "omits a highly material fact" -that the request is aimed at obtaining information which may be used to impeach the witness in litigation.<sup>8</sup> The Philadelphia opinion further recognizes, as does this Committee, that the witness would not likely accept the social media request if the witness knew its true origin and context. An opinion from the San Diego County Bar Association reaches the same conclusion. San Diego Cty. Bar Legal Ethics Op. 2011-2. The Committee finds that the San Diego and Philadelphia opinions are consistent with the New Hampshire Rules of Professional Conduct but that the New York City opinion is not. A lawyer has a duty to investigate but also a duty to do so openly and honestly, rather than through subterfuge.

Finally, this situation should be distinguished from the situation where a person, not acting as an agent or at the behest of the lawyer, has obtained information from the witness's social media account. In that instance, the lawyer may receive the information and use it in litigation as any other information. The difference in this latter context is that there was no deception by the lawyer. The witness chose to reveal information to someone who was not acting on behalf of the lawyer. The witness took the risk that the third party might repeat the information to others. Of course, lawyers must be scrupulous and honest, and refrain from expressly directing or impliedly sanctioning someone to act improperly on their behalf. Lawyers are barred from violating the rules "through the acts of another." Rule 8.4(a).

#### CONCLUSION

As technology changes, it may be necessary to reexamine these conclusions and analyze new situations. However, the basic principles of honesty and fairness in dealing with others will remain the same. When lawyers are faced with new concerns regarding social media and communication with witnesses, they should return to these basic principles and recall the Supreme Court's admonition that honesty is the most important guiding principle of the bar in New Hampshire.

---

**SOURCES/AUTHORITIES**

**Opinions**

- New York City Bar Association, Formal Opinion 2012-2
- New York City Bar Association, Formal Opinion 2010-2
- New York State Bar Association, Opinion #843 (9/10/2010)
- The Philadelphia Bar Association, Professional Guidance Committee, Opinion 2009-02, (March 2009)
- San Diego County Bar Legal Ethics Committee, Legal Ethics Opinion 2011-2

**Other Sources**

- McManus, "Friending" Adverse Witnesses: When Does It Cross The Line Into Unethical Conduct, Lexis Hub – Law, Technology, and Social Media (February 2011).
- Lackey and Minta, Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging, 28 Touro Law Review 149 (July 2012).
- Strutin, Social Media and the Vanishing Points of Ethical and Constitutional Boundaries, 31 Pace Law Review 228 (Winter 2011).
- Cook and Tsao, Using Social Media As A Tool In Litigation: An Overview Of Evidentiary And Ethical Considerations, ABA Section of Labor and Employment Law, 6th Annual Labor and Employment Law Conference, October 31 – November 3, 2012.

---

**ENDNOTES**

- <sup>1</sup> In the remainder of this opinion, the Committee refers to this as a communication "in-name-only."
- <sup>2</sup> See, e.g., *Thomas v. Kuhlman*, 255 F. Supp. 2d 99, 107 (E.D.N.Y.2003); *Williams v. Washington*, 59 F.3d 673, 680-81 (7th Cir. 1995); *People v. Donovan*, 184 A.D.2d 654, 655 (N.Y. App. Div. 1992); see also American Bar Association Criminal Justice Standards, Defense Function §4-4.1.
- <sup>3</sup> For the purposes of this opinion, an unrestricted page is a page which may be viewed without the owner's authorization but which may require membership with the same social media service.
- <sup>4</sup> "Facebook by the Numbers: 1.06 Billion Monthly Active Users," [available online](#).
- <sup>5</sup> San Diego County Bar Legal Ethics Committee, Legal Ethics Opinion 2011-2; NY Bar Ethics Op. #843 (9/10/2010).
- <sup>6</sup> San Diego County Bar Legal Ethics Committee, Legal Ethics Opinion 2011-2; Phil. Bar Assoc., Prof. Guidance Comm., Op. 2009-02.
- <sup>7</sup> Pursuant to ABA Ethics Opinion 11-461, a lawyer may advise a client regarding the client's right to communicate directly with the other party in the legal matter and assist the client in formulating the substance of any proposed communication, so long as the lawyer's conduct falls short of overreaching. This opinion has engendered significant controversy because, according to some critics, it effectively allowed the lawyer to "script" conversations between the client and a represented opposing party and prepare documents for the client to deliver directly to the represented opponent. For a more complete discussion, see Podgers, On Second Thought: Changes Muled Re ABA Opinion on Client Communications Issue, ABA Journal (Jan. 1, 2012), [available online](#) (last accessed May 22, 2013). The Committee takes no position on this issue and cites the opinion solely to illustrate the point that the client may independently obtain and share information with the lawyer, subject to certain constraints.
- <sup>8</sup> In contrast to this opinion, the Philadelphia opinion does not find a violation of Rule 4.3.

<b>ADDRESS CHANGE?</b>	Supreme Court Rule 42(9) requires all NH admitted attorneys to notify the Bar Association of any address change, home or office.	<b>RETURN —TO— SENDER</b>
----------------------------	--	-----------------------------------

[Home](#) | [About the Bar](#) | [For Members](#) | [For the Public](#) | [Legal Links](#) | [Publications](#) | [Online Store](#)  
[Lawyer Referral Service](#) | [Law-Related Education](#) | [NHBA-CLE](#) | [NHBA Insurance Agency](#) | [NHMCLE](#)  
[Search](#) | [Calendar](#)

New Hampshire Bar Association  
2 Pillsbury Street, Suite 300, Concord NH 03301  
phone: (603) 224-6942 fax: (603) 224-2910  
email: [NHBAinfo@nhbar.org](mailto:NHBAinfo@nhbar.org)  
© NH Bar Association [Disclaimer](#)

## Ethics Opinion 370

## Social Media I: Marketing and Personal Use

## Introduction

Social media and social networking websites are online communities that allow users to share information, messages, and other content, including photographs and videos. The Committee defines social media as follows:

Social media include any electronic platform through which people may communicate or interact in a public, semi-private or private way. Through blogs, public and private chat rooms, listservs, other online locations, social networks and websites such as Facebook, LinkedIn, Instagram, Twitter, Yelp, Angie's List, Avvo and Lawyers.com, users of social media can share information, messages, e-mail, instant messages, photographs, video, voice or videoconferencing content.[1] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn1) This definition includes social networks, public and private chat rooms, listservs, and other online locations where attorneys communicate with the public, other attorneys, or clients. Varying degrees of privacy may exist in these online communities as users may have the ability to limit who may see their posted content and who may post content to their pages.[2] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn2)

Increasingly, attorneys are using social media for business and personal reasons. The Committee wants to raise awareness of the benefits and pitfalls of the use of social media within the practice of law and to emphasize that the District of Columbia Rules of Professional Conduct (the "Rules") apply to attorneys in the District of Columbia (the "District") who use, or may use, social media for business or personal reasons.[3] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn3) This Opinion applies to all attorneys who use social media, regardless of practice area or employer and applies regardless of whether the attorney engages in advertising or client communications via social media. The Committee notes that any social media presence, even a personal page, could be considered advertising or marketing, and lawyers are cautioned to consider the Rules applicable to attorney advertising, even if not explicitly discussed below. Lawyers reviewing this Opinion may also wish to review Opinion 371 (Social Media II), which addresses use of social media by lawyers in providing legal services.

Social networking websites provide an online community for people to share daily activities, their interests in various topics, or to increase their circle of personal or business acquaintances. There are sites with primarily business purposes, some that are primarily for personal use and some that offer a variety of different uses. According to the 2014 ABA Legal Technology Survey, among attorneys and law firms, in addition to blogs, LinkedIn, Facebook and Twitter are among the more widely used social networks.[4] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn4) On these sites, members create online "profiles," which may include biographical data, pictures and other information that they wish to post. These services permit members to locate and invite other members of the network into their personal networks (to "connect" or "friend" them) or to invite the friends or contacts of others to connect with them.

Members of these online social networking communities communicate in a number of ways, publicly or privately. Members of these online social networking communities may have the ability, in many instances, to control who may see their posted content, or who may post content to their pages. Varying degrees of privacy exist. These privacy settings allow users to restrict or limit access of information to certain groups, such as "friends," "connections" or the "public."

Social media sites, postings or activities that mention, promote or highlight a lawyer or a law firm are subject to and must comply with the Rules.[5] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn5) Attorneys who choose to use social media must adhere to the Rules in the same way that they would if using more traditional forms of communication.

The Rules, as well as previous Opinions of this Committee, apply to a number of different social media or social networking activities that an attorney or law firm may be engaged in, including:

1. Connecting and communicating with clients, former clients or other lawyers on social networking sites;
2. Writing about an attorney's own cases on social media sites, blogs or other internet-publishing based websites;
3. Commenting on or responding to online reviews or comments;
4. Self-identification by attorneys of their own "specialties," "skills" and "expertise" on social media sites;
5. Reviewing third-party endorsements received by attorneys on their personal or law firm pages; and,
6. Making endorsements of other attorneys on social networking sites.

The Committee concludes that, generally, each of the activities identified above are permissible under the Rules; but not without caution, as discussed in greater detail below. Consistent with our mandate, we consider only the applicability of the D.C. Rules of Professional Conduct. Given that social media does not stop at state boundaries, we remind members of the District of Columbia Bar that their social media presence may be subject to regulation in other jurisdictions, either because the District applies another state's rules through its choice-of-law rule.[6] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn6) or because other states assert jurisdiction over attorney conduct without regard to whether the attorney is admitted in other states.[7] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn7)

Lawyers must be aware of the ethical rules regarding social media in the principal jurisdiction where they practice, consistent with Rule 8.5. However, adherence to the ethical rules in the jurisdiction of one's principal practice may not insulate an attorney from discipline. There is considerable variation in choice of law rules across jurisdictions. We specifically wish to caution lawyers that the disciplinary rules of other jurisdictions, including our neighboring jurisdictions of Maryland and Virginia, allow for the imposition of discipline upon attorneys who are not admitted in that jurisdiction, if the lawyer provides or offers to provide any legal services in the jurisdiction. ABA Model Rule 8.5(b)(2) provides a limited safe harbor to this provision, by stating that "[a] lawyer shall not be subject to discipline if the lawyer's conduct conforms to the rules of a jurisdiction in which the lawyer reasonably believes the predominant effect of the lawyer's conduct will occur." We note, however, that not every state has adopted this safe harbor. This Committee undertook a detailed evaluation of choice of law rules in non-judicial proceedings in Opinion 311.[8] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn8)

We explicitly note that this Opinion is limited to the use of social media as a communications device. This Opinion does not address issues related to the ethical use of social media in litigation or other proceedings, or with regard to issues related to advising clients on the use of social media. Those issues are addressed in Opinion 371 (Social Media II).

## Applicable Rules

The Rules that are potentially implicated by social media include:

- Rule 1.1 (Competence)
- Rule 1.6 (Confidentiality of Information)
- Rule 1.7 (Conflict of Interest: General)
- Rule 1.7 (Duties to Prospective Client)
- Rule 1.18 (Duties to Prospective Client)
- Rule 3.3 (Candor to Tribunal)
- Rule 5.1 (Responsibilities of Partners, Managers, and Supervisory Lawyers)
- Rule 5.3 (Responsibilities Regarding Non-Lawyer Assistants)
- Rule 7.1 (Communications Concerning a Lawyer's Services)
- Rule 8.4 (Misconduct)
- Rule 8.5 (Disciplinary Authority; Choice of Law)

## Discussion

## I. Social Media In General

The guiding principle for lawyers with regard to the use of any social network site is that they must be conversant in how the site works. Lawyers must understand the functionality of the social networking site, including its privacy policies. Lawyers must understand the manner in which postings on social media sites are made and whether such postings are public or private. Indeed, comment [6] to Rule 1.1 (Competence) provides:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and engage in such continuing study and education as may be necessary to maintain competence.

As discussed in more detail herein, lawyers must be cognizant of the benefits and risks of the use of social media and their postings on social media sites. Social networking sites, and social media in general, make it easier to blur the distinctions between communications that are business and those that are personal. Communications via social media are inherently less formal than more traditional or established forms of communication. Lawyers and law firm employees must be reminded of the need to maintain confidentiality with regard to clients and client matters in all communications. It is recommended that all law firms have a policy in place regarding employees' use of social networks. Lawyers in law firms have an ethical duty to supervise subordinate lawyers and non-lawyer staff to ensure that their conduct complies with the applicable Rules, including the duty of confidentiality. See Rules 5.1 and 5.3.

Content contained on a lawyer's social media pages must be truthful and not misleading. Statements on social media could expose an attorney to charges of dishonesty under Rule 8.4 or lack of candor under Rule 3.3, if the social media statements conflict with statements made to courts, clients or other third parties, including employers. Similarly, statements on social media could expose a lawyer to civil liability for defamation, libel or other torts.

**II. Permissible Uses of Social Media**

**A. Attorneys may connect with and communicate with clients, former clients or other lawyers on social networking sites, but not without caution.**

There are no provisions of the Rules that preclude a lawyer from participating in social media or other online activities. However, if an attorney connects with, or otherwise communicates with clients on social networking sites, then the attorney must continue to adhere to the Rules and maintain an appropriate relationship with clients. Lawyers must also be aware that, if they are connected to clients or former clients on social media, then content made by others and then placed on the attorney's page and content made by the attorney may be viewed by these clients and former clients. Attorneys should be mindful of their obligations under Rule 1.6 to maintain client confidences and secrets.

Some social networking sites, like Facebook, offer users the option to restrict what some people may see on a user's page. These options also allow a user to determine who may post content publicly on the lawyer's page. It is advisable for lawyers to periodically review these settings and adjust them as needed to manage the content appearing publicly on the lawyer's social media pages. Attorneys should be aware of changes to the policies of the sites that they utilize, as privacy policies are frequently changed and networks may globally apply changes, pursuant to the updated policies.

**I. Avoiding the formation of an inadvertent attorney-client relationship**

As we opined in Opinion 316, it is permissible for lawyers to participate in online chat rooms and similar arrangements through which attorneys could engage in real time, or nearly real time communications with Internet users. However, that permission was caveated with the caution to avoid the provision of specific legal advice in order to prevent the formation of an attorney-client relationship. In Opinion 302, we provided "best practices" guidance on Internet communications, with the intent of avoiding the inadvertent formation of an attorney-client relationship. One of the suggested "best practices" included the use of a prominent disclaimer. *Id.* However, we have reiterated "that even the use of a disclaimer may not prevent the formation of an attorney-client relationship if the parties' subsequent conduct is inconsistent with the disclaimer." D.C. Ethics Op. 316.

These same principles are applicable to the use of social media. Disclaimers are advisable on social media sites, especially if the lawyer is posting legal content or if the lawyer may be engaged in sending or receiving messages from "friends," whether those friends are other attorneys, family or unknown visitors to the lawyer's social media page, when those messages relate, or may relate, to legal issues. [9] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn9](#))

Rule 1.18 imposes a duty of confidentiality with regard to a prospective client, who is defined in Rule 1.18(a) as "a person who discusses ... the possibility of forming a client-lawyer relationship with respect to a matter." However, comment [2] to Rule 1.18 notes that "[a] person who communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship, is not a 'prospective client' within the meaning of [the Rule]." The guidance of Rule 1.18 is of particular importance in social networking, where lawyers may self-identify themselves as attorneys and where, most likely, those "connected" to the lawyer will be aware that the user is an attorney; however, without more, the mere knowledge that a friend is an attorney does not give rise to a reasonable expectation that interactions with that attorney would create a prospective or actual client relationship, or its attendant duty of confidentiality.

**II. Avoiding the creation of conflicts of interest**

Consideration must also be given to avoid the acquisition of uninvited information through social media sites that could create actual or perceived conflicts of interest for the lawyer or the lawyer's firm. Caution should be exercised when stating positions on issues, as those stated positions could be adverse to an interest of a client, thus inadvertently creating a conflict. Rule 1.7(b)(4) states that an attorney shall not represent a client with respect to a matter if "the lawyer's professional judgment on behalf of the client will be or reasonably may be adversely affected by ... the lawyer's own financial, business, property or personal interests," unless the conflict is resolved in accordance with Rule 1.7(c). Content of social media posts made by attorneys may contain evidence of such conflicts.

Moreover, online communications and interactions with people who are unknown to the lawyer may unintentionally cause the development of relationships with persons or parties who may have interests that are adverse to those of existing clients.

**III. Protecting client confidences and secrets**

Protecting client information is of the utmost importance when using social media. Most attorneys are aware of the importance of protecting attorney-client communications, attorney work-product or other privileged information. The obligation to protect this information extends beyond the termination of the attorney-client relationship.

Rule 1.6 distinguishes between information that is "confidential" and that which is a "secret," and requires attorneys to protect both kinds of information. In the District of Columbia,

"Confidence" refers to information protected by the attorney-client privilege under applicable law. "Secret" refers to other information gained in the professional relationship that the client has requested be held inviolate, or the disclosure of which would be embarrassing, or would be likely to be detrimental, to the client.

Rule 1.6(b). Comment [8] to Rule 1.6 makes clear that the Rule potentially applies to all information gained in the course of the professional relationship, and exists without regard to the nature or source of the information, or the fact that others share the knowledge.

No less critical are considerations of the level of confidentiality available on the social media sites themselves. If an attorney uses social media to communicate with potential or actual clients or co-counsel, then careful attention must be paid to issues of privacy and confidentiality. It is critically important that lawyers review the policies of the social media sites that they frequent, particularly policies related to data collection. Privacy settings on social media are not the equivalent of a guarantee of confidentiality.

Particular consideration must be given to the issue of maintaining and protecting the confidentiality of communications on social networking sites. [10] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn10](#)) Messaging and electronic mail services provided by social networking sites may lack safeguards sufficient for communicating with clients or prospective clients. Moreover, the messaging and electronic mail services provided by these sites should not be assumed to be confidential or private. Therefore, when appropriate, clients or potential clients should be advised by lawyers of the existence of more secure means of communicating confidential, privileged, sensitive or otherwise protected information. Messages with clients that are sent or received via social networks must be treated with the same degree of reasonable care as messages sent or received via electronic mail or other traditional means of communication. Social media sites may not permanently retain messages or other communications; therefore care should be taken to preserve these communications outside of the social media site, in order to ensure that the communications are maintained as part of the client file. It is advisable that communications regarding on-going representations or pending legal matters be made through secured office e-mail, and not through social media sites.



Certain social media sites collect information about the people and groups that the user is connected to and the interactions with that group or person. The information collected is gathered from both the lawyer and the person communicating with the lawyer and can include content, information and frequency of contact.<sup>[11]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn11](#)) These sites also collect information about uses of their partner products and/or websites, allowing the social media service to collect and integrate information about its users, which can be used for targeted advertising and/or research purposes.<sup>[12]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn12](#)) Thus, depending on the intended use of the social media site, it is advisable for a lawyer to give careful consideration to which social media sites, if any, may be more appropriate for business-related uses or for communications with potential or actual clients.

When inviting others to view a lawyer's social media site, or profile, a lawyer must be mindful of the ethical restrictions relating to solicitations and other communications. Most social networking sites require an e-mail address from the user as part of the registration process. Then, once the social networking site is accessed by a lawyer, the site may access the entire address book (or contacts list) of the user. Aside from any data collection purposes, this access allows the social media site to suggest potential connections with people the lawyer may know who are already members of the social network, to send requests or other invitations to have these contacts connect with the lawyer on that social network, or to invite non-members of the social network to join it and connect with the lawyer.

However, in many instances, the people contained in a lawyer's address book or contact list are a blend of personal and professional contacts. Contact lists frequently include clients, opposing counsel, judges and others whom it may be impermissible, inappropriate or potentially embarrassing to have as a connection on a social networking site. The connection services provided by many social networks can be a good marketing and networking tool, but for attorneys, these connection services could potentially identify clients or divulge other information that a lawyer might not want an adversary or a member of the judiciary to see or information that the lawyer is obligated to protect from disclosure. Accordingly, great caution should be exercised whenever a social networking site requests permission to access e-mail contacts or to send e-mail to the people in the lawyer's address book or contact list and care should be taken to avoid inadvertently agreeing to allow a third-party service access to a lawyer's address book or contacts.

**B. Attorneys may write about their own cases on social media sites, blogs or other Internet-based publications, with the informed consent of their clients.**

The scope of the protections provided in Rule 1.6 militates in favor of prudence when it comes to disclosing information regarding clients and cases. While lawyers may ethically write about their cases on social media, lawyers must take care not to disclose confidential or secret client information in social media posts. Rule 1.6(e)(1) states that a lawyer may use a client's confidences and secrets for the lawyer's own benefit or that of a third party only after the attorney has obtained the client's informed consent to the use in question. Because Rule 1.6 extends to even information that may be known to other people, the prudent lawyer will obtain client consent before sharing any information regarding a representation or disclosing the identity of a client. Even if the attorney is reasonably sure that the information being disclosed would not be subject to Rule 1.6, it is prudent to obtain explicit informed client consent before making such posts. With or without client consent, attorneys should exercise good judgment and great caution in determining the appropriateness of such posts. Consideration should be given to the identity of the client and the sensitivity of the subject matter, even if the client is not overtly identified. It is advisable that the attorney share a draft of the proposed post or blog entry with the client, so there can be no miscommunication regarding the nature of the content that the attorney wishes to make public. It is also advisable, should the client agree that the content may be made public, that the attorney obtain that client consent in a written form.

Consideration must also be given to ensure that such disclosures on social media are compliant with Rule 7.1. Rule 7.1 governs all communications about a lawyer's services, including advertising. These Rules extend to online writings, whether on social media, a blog or other Internet-based publication, regarding a lawyer's own cases. Such communications are subject to the Rules because they have the capacity to mislead by creating the unjustified expectation that similar results can be obtained for others. Care must be taken to avoid material misrepresentations of law or fact, or the omission of facts necessary to make the statement considered as a whole not materially misleading. Accordingly, social media posts regarding a lawyer's own cases should contain a prominent disclaimer making clear that past results are not a guarantee that similar results can be obtained for others.

Law firms that have blogs or social media sites or that allow their lawyers to maintain their own legal blogs or social media pages should take appropriate steps to ensure that such content is compliant with the Rules, consistent with the duties set forth in Rule 5.1. Non-attorney employees who create content for their own or their employers' social media sites should be educated regarding the protection of client information and, if appropriate, be supervised by their employing law firm or lawyer, as required by Rule 5.3.<sup>[13]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn13](#))

As noted above, all social media postings for law firms or lawyers, including blogs, should contain disclaimers and privacy statements sufficient to convey to prospective clients and visitors that the social media posts are not intended to convey legal advice and do not create an attorney-client relationship.

**C. Attorneys may, with caution, respond to comments or online reviews from clients.**

The ability for clients to place reviews and opinions of the services provided by their counsel on the Internet can present challenges for attorneys. An attorney must monitor his or her own social networking websites, verify the accuracy of information posted by others on the site, and correct or remove inaccurate information displayed on their social media page(s). As set forth in comment [1] to Rule 7.1, client reviews that may be contained on social media posts or webpages must be reviewed for compliance with Rule 7.1(a) to ensure that they do not create the "unjustified expectation that similar results can be obtained for others."<sup>[14]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn14](#))

Attorneys may respond to negative online reviews or comments from clients. However, Rule 1.6 does not provide complete safe harbor for the disclosure of client confidences in response to a negative internet review or opinion. Rule 1.6(e) states that:

A lawyer may use or reveal client confidences or secrets:

(3) to the extent reasonably necessary to establish a defense to a criminal charge, disciplinary charge, or civil claim, formally instituted against the lawyer, based upon conduct in which the client was involved, or to the extent reasonably necessary to respond to specific allegations by the client concerning the lawyer's representation of the client [emphasis added].

Thus, the lawyer's ability to reveal confidences under Rule 1.6(e)(3) is limited to only "specific" allegations by the client concerning the lawyer's representation of the client. Comment [25] to Rule 1.6 specifically excludes general criticisms of an attorney from the kinds of allegations to which an attorney may respond using information otherwise protected by Rule 1.6. However, even when the lawyer is operating within the scope of the Rule 1.6(e)(3) exception, the comments to Rule 1.6 caution that disclosures should be no greater than the lawyer reasonably believes are necessary. There is no exception in Rule 1.6 that allows an attorney to disclose client confidences or secrets in response to specific or general allegations regarding an attorney's conduct contained in an online review from a third party, such as opposing counsel or a non-client.<sup>[15]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn15](#))

Other jurisdictions have taken a more restrictive view of responding to comments or reviews on lawyer-rating websites. For example, the New York State Bar Association Committee on Professional Ethics, in its Opinion 1032 (2014), held that "[a] lawyer may not disclose confidential client information solely to respond to a former client's criticism of the lawyer posted on a [lawyer-rating website]." The New York analysis turned on the language contained in New York's Rule 1.6, which requires "accusations," rather than allegations. In order to trigger the "self-defense" exception of N.Y. Rule 1.6, Attorneys licensed in the District of Columbia who are admitted to practice in multiple jurisdictions are cautioned that they may be subject to the disciplinary authority of both this jurisdiction and another jurisdiction where the lawyer is admitted for the same conduct. Under the District's choice of law rule, Rule 8.5(b)(2)(ii),

the rules to be applied shall be the rules of the admitting jurisdiction in which the lawyer principally practices; provided, however, that if particular conduct clearly has its predominant effect in another jurisdiction in which the lawyer is licensed to practice, the rules of that jurisdiction shall be applied to that conduct.

See notes 6 and 7, *infra*.<sup>[16]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn16](#))

We recognize that there are limitations on the control that any individual can assert over his or her presence on the Internet. That is why we recognize that an attorney's ethical obligations to review and regulate content on social media extends only to those social media sites or webpages for which the attorney maintains control of the content, such as the ability to delete posted content, block users from posting, or block users from viewing. However, notwithstanding the scope of the attorney's affirmative obligations, it is highly advisable for attorneys to be aware of content regarding them on the Internet.

**D. An attorney or law firm may identify "specialties," "skills" and "expertise" on social media, provided that the representations are not false or misleading.**

Many social media sites, like LinkedIn, allow attorneys to identify skills and areas of practice. The District of Columbia does not prohibit statements regarding specialization or expertise. Accordingly, District of Columbia attorneys are ethically permitted to identify their skills, expertise and areas of practice, subject to Rule 7.1(a).<sup>[17]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn17](#))

As we previously opined in Opinion 249, "Rule 7.1(a) permits truthful claims of lawyer specialization so long as they can be substantiated." Rule 7.1(a) states that an attorney is prohibited from making a "false or misleading communication about the lawyer or the lawyer's services." The relevant comment [1] to this Rule states that "[i]t is especially important that statements about a lawyer or the lawyer's services be accurate, since many members of the public lack detailed knowledge of legal matters." Accordingly, we conclude that social media profiles or pages that include statements by the attorney setting forth an attorney's skills, areas of specialization or expertise are subject to Rule 7.1(a) and, therefore, cannot be false or misleading.

**E. Attorneys must review their social media presence for accuracy.**

Consistent with the goals of networking, marketing and making connections, some social networking sites permit members of the site to recommend fellow members or to endorse a fellow member's skills. Users may also request that others endorse the lawyer for specified skills that the lawyer has indicated he or she possesses. LinkedIn and other sites also allow clients or others to submit written reviews or recommendations of the lawyer. Other legal-specific social networking sites focus exclusively on endorsements or recommendations. It is our view that a lawyer is ethically permitted, with caution, to recommend other attorneys, and to accept endorsements, written reviews and recommendations, subject to the Rules.

As noted above, it is our opinion that lawyers in the District of Columbia have a duty to monitor their social network sites. If a lawyer controls or maintains the content contained on a social media page, then the lawyer has an affirmative obligation to review the content on that page. A lawyer must remove endorsements, recommendations or other content that are false or misleading. Lawyers are advised that it is appropriate to reject or refuse endorsements from people who lack the knowledge necessary for making the recommendation. It would be misleading for an attorney to display recommendations or endorsements of skills that are received from people who do not have a factual basis to evaluate the lawyer's skills. Lawyers must reject or refuse endorsements that indicate that the lawyer possesses skills or expertise that the lawyer does not possess. It would be misleading for an attorney to display a recommendation that contained incorrect information. The operative questions asked by the lawyer when reviewing endorsements or recommendations received on their social media pages should be whether the person making the endorsement knows the lawyer and whether the person can fairly comment on the lawyer's skills.

We recommend that lawyers who are using social media sites that allow for the review of posts, recommendations or endorsements prior to publication avail themselves of the settings that allow review and approval of such information before it is publicized on the lawyer's social media page. Some sites, like LinkedIn, provide settings that allow the user to review and approve endorsements that are received before the endorsements are posted publicly. Users may also choose to keep endorsements hidden so that they are not seen by others.<sup>[18]</sup> ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fn18](#)) Other social networking sites, like Facebook, allow users to adjust their privacy settings to require user approval before certain content, such as photos, can be displayed on a user's home page. Some social media sites allow users to adjust their privacy settings to require approval before a user can be "tagged," a practice that allows content on another person's page to be displayed on the user's page.

It is suggested that lawyers, particularly those who do not frequently monitor their social media pages, those who may not know everyone in their networks well, or those who wish to have an added layer of protection, utilize these heightened privacy settings. Aside from the potential ethical issues discussed herein, there are many good reasons for a lawyer to want to maintain a higher level of control over what content others may place on a lawyer's social media page(s).

It is permissible under the Rules for a lawyer to make an endorsement or recommendation of another attorney on a social networking site, provided that the endorsement or recommendation is not false or misleading. Such endorsements and recommendations must be based upon the belief that the recipient of the endorsement does in fact possess said skills or legal acumen. Rule 8.4(c) prohibits an attorney from being dishonest, or engaging in fraud, deceit or misrepresentation. Therefore, a lawyer must only provide an endorsement or recommendation of someone on social media that the endorsing lawyer believes to be justified.

Rule 8.4(a) states that it is misconduct for a lawyer to violate or to attempt to violate ethics rules through the acts of others. Thus, clients and colleagues cannot say things about the lawyer that the lawyer cannot say. The lawyer's obligation to monitor, review and correct content on social media sites for which they maintain control exists regardless of whether the information was posted by the attorney, a client or a third party.

We reiterate that, for websites or social media sites where the attorney does not have editorial control over content of the postings of others, we do not believe that the Rules impose an affirmative duty on a lawyer to monitor the content of the sites; however, under certain circumstances, it may be appropriate for the attorney to request that the poster remove the content, to request that the social networking site remove the content, or for the attorney to post a curative response addressing the inaccurate content.

**Conclusion**

Social media is a constantly changing area of technology. Social media can be an effective tool for providing information to the public, for networking and for communications. However, using such tools requires that the lawyer maintain and update his or her social media pages or profiles in order to ensure that information is accurate and adequately protected.

Accordingly, this Committee concludes that a lawyer who chooses to maintain a presence on social media, for personal or professional reasons, must take affirmative steps to remain competent regarding the technology being used and to ensure compliance with the applicable Rules of Professional Conduct.

The world of social media is a nascent area that continues to change as new technology is introduced into the marketplace. Best practices and ethical guidelines will, as a result, continue to evolve to keep pace with such developments.

[1] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref1](#)) "Content" means any communications, whether for personal or business purposes, disseminated through websites, social media sites, blogs, chat rooms, listservs, instant messaging, or other internet presences, and any attachments or links related thereto.

[2] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref2](#)) The Merriam-Webster Dictionary defines "social media" as "forms of electronic communication ... through which users create online communities to share information, ideas, personal messages, and other content..." More specifically to the legal profession, the New York State Bar Association Committee on Professional Ethics, in its Formal Opinion No. 2012-2 (May 30, 2012), stated:

We understand "social media" to be services or websites people join voluntarily in order to interact, communicate, or stay in touch with a group of users, sometimes called a "network." Most such services allow users to create personal profiles, and some allow users to post pictures and messages about their daily lives.

[3] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref3](#)) We have previously addressed issues related to attorneys' participation in certain kinds of internet and electronic communications, but have not yet addressed the broader uses of social media. In Opinion 316, we concluded that attorneys could take part in online chat rooms and similar arrangements through which they could engage in communications in real time or nearly real time, with internet users seeking legal information. D.C. Legal Ethics Op. 316 (2002). In Opinion 281, we addressed issues related to the use of unencrypted electronic mail. D.C. Legal Ethics Op. 281 (1999). In Opinion 302, we stated that lawyers could use websites to advertise for plaintiffs for class action lawsuits and use websites that offer opportunities to bid competitively on legal projects. D.C. Legal Ethics Op. 302 (2000).

[4] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref4](#)) [www.americanbar.org/publications/techreport/2014/blogging-and-social-media.html](http://www.americanbar.org/publications/techreport/2014/blogging-and-social-media.html) ([javascrip:HandleLink](#) ([?page=0\\_0;CPNEWWIN:blank\\*top=10,left=10,width=300,height=300,toolbar=1,location=1,directories=1,status=1,menuubar=1,scrollbars=1,resizable=1@http://www.and-social-media.html](#));) (last visited Oct. 26, 2016).

[5] ([/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref5](#)) The Committee further notes that even social media profiles that are used exclusively for personal purposes might be viewed by clients or other third parties, and that information contained on those social media websites may be subject to the Rules of Professional Conduct. The Rules extend to purely private conduct of a lawyer, in areas such as truthfulness and compliance with the law. See Rule 8.4.

[6] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref6) In accordance with D.C. Rule 8.5(b), the Office of Disciplinary Counsel will apply the rules of another jurisdiction to an attorney's conduct in two circumstances:

- (1) For conduct in connection with a matter pending before a tribunal, the rules to be applied shall be the rules of the jurisdiction in which the tribunal sits, unless the rules of the tribunal provide otherwise, and
- (2) For any other conduct, . . .
  - (i) If the lawyer is licensed to practice in this and another jurisdiction, the rules to be applied shall be the rules of the admitting jurisdiction in which the lawyer principally practices; provided, however, that if particular conduct clearly has its predominant effect in another jurisdiction in which the lawyer is licensed to practice, the rules of that jurisdiction shall be applied to that conduct.

Note that, in contrast to ABA Model Rule 8.5 (see *infra* note 7), D.C. Rule 8.5 does not provide for jurisdiction over attorneys not admitted to practice in the District and does not apply the rules of another jurisdiction unless the attorney is either practicing before a tribunal in another jurisdiction, or is licensed to practice in another jurisdiction.

[7] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref7) In contrast to D.C. Rule 8.5 (discussed *supra* in note 6), ABA Model Rule 8.5(a) states that "[a] lawyer not admitted in this jurisdiction is also subject to the disciplinary authority of this jurisdiction if the lawyer provides or offers to provide any legal services in this jurisdiction." Moreover, ABA Model Rule 8.5(b)(2) states that for conduct not in connection with a matter pending before a tribunal, the rules to be applied are "the rules of the jurisdiction in which the lawyer's conduct occurred, or, if the predominant effect of the conduct is in a different jurisdiction, the rules of that jurisdiction shall be applied to the conduct." Accordingly, Model Rule 8.5(b)(2), unlike D.C. Rule 8.5(b)(2), may result in the application of rules of jurisdictions to which the lawyer is not admitted.

[8] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref8) D.C. Legal Ethics Op. 311 (2002). The revisions to Rule 8.5(b)(1) that became effective on February 1, 2007 have modified Opinion 311 to the extent that the Opinion now applies more broadly to conduct in connection with a "matter pending before a tribunal" rather than only in connection with a "proceeding in a court before which a lawyer has been admitted to practice." These revisions, however, do not change this Committee's analysis in Opinion 311 as to "other conduct" under Rule 8.5(b)(2).

[9] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref9) As we discussed in Opinion 302, in the District of Columbia, the question of what conduct gives rise to an attorney-client relationship is a matter of substantive law. Neither a retainer nor a formal agreement is required in order to establish an attorney-client relationship in the District of Columbia. See, e.g., *In re Lieber*, 442 A.2d 153 (D.C. 1982) (attorney-client relationship formed where attorney failed to indicate lack of consent to accept a court appointed client after receiving notification of appointment by mail). Further, even casual legal advice can give rise to an attorney-client relationship if the putative client relies upon it. See, e.g., *Togstad v. Vesely, Otto, Miller & Keffe*, 291 N.W.2d 686 (Minn. 1980) (finding an attorney-client relationship where the attorney stated that he did not think a prospective client had a cause of action but would discuss it with his partner, did not call prospective client back, and prospective client relied on attorney's assessment and did not continue to seek legal representation).

[10] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref10) See also D.C. Legal Ethics Op. 281.

[11] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref11) An example is contained in Facebook's data policy. (<https://www.facebook.com/about/privacy/> ([javascript:HandleLink\(cpe\\_0\\_0'CPNEWWIN: blank\\*@https://www.facebook.com/about/privacy/\);](https://www.facebook.com/about/privacy/)) (last visited Oct. 26, 2016).

[12] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref12) Miller, C., *The Plus in Google Plus? It's Mostly for Google*, Feb. 14, 2014 [http://www.nytimes.com/2014/02/15/technology/the-plus-in-google-plus-its-mostly-for-google.html?\\_r=0](http://www.nytimes.com/2014/02/15/technology/the-plus-in-google-plus-its-mostly-for-google.html?_r=0) ([javascript:HandleLink\(cpe\\_0\\_0'CPNEWWIN: blank\\*@https://www.nytimes.com/2014/02/15/technology/the-plus-in-google-plus-its-mostly-for-google.html?\\_r=0'\);](https://www.facebook.com/about/privacy/)) (last visited Oct. 26, 2016).

[13] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref13) See, e.g., Gene Shipp, *Bar Counsel: 20/20: The Future of the Rules of Professional Conduct*, WASHINGTON LAWYER (June 2013), sharing the example that our world is changing so fast that "a high-profile celebrity, who comes to your office on a highly confidential matter and graciously pauses to allow a picture with your receptionist, may be unhappy with your staff's violation of Rule 1.6 when their picture appears on the Internet even before you have had a chance to say hello."

[14] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref14) The Committee does not distinguish between client comments that are solicited and those that are unsolicited. Rule 7.1 governs all communications about a lawyer's services.

[15] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref15) Although beyond the scope of this Opinion, the Committee notes that the Rule 1.6(e)(3) exception allows an attorney to respond to wrongs alleged by a third party, but only if the third party has formally instituted a civil, criminal or disciplinary action against the lawyer. See comments [23] and [24] to Rule 1.6.

[16] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref16) Other jurisdictions have sanctioned attorneys for disclosures of client confidences or secrets on social media or other websites. In 2013, the Hearing Board of the Illinois Attorney Registration and Disciplinary Commission held, in the *Matter of Betty Tsamis*, that it was a violation of Rule 1.6(a) for an attorney to respond to an unfavorable review on the legal referral website AVVO with a response that revealed confidential information about the client's case. In *Tsamis*, the attorney first requested that the client remove the posting from the website, which is also a permissible response in the District of Columbia. The client responded that he would remove the post, but only if the attorney returned his files and refunded his fees. Thereafter, AVVO removed the posting from its online client reviews. The client then posted a second negative client review to the same website, which the attorney responded to, disclosing client information. The Hearing Board found that the response exceeded what was necessary to respond to the client's accusations and a reprimand was recommended.

[17] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref17) Prudent attorneys should consider the most restrictive rules applicable to them when using self-promotional features on social media. We note that other jurisdictions, like New York, do not permit lawyers to identify themselves as "specialists" unless they have been certified as such by an appropriate organization. They are, however, permitted to detail their skills and experience. See N.Y. Cnty. Lawyers Ass'n Comm. on Prof'l Ethics, Op. 748 (Mar. 10, 2015).

[18] (/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm#fnref18) Lawyers are advised to review the guidance provided by other jurisdictions in which they are admitted to practice regarding the use of endorsements or the skills and expertise sections in a LinkedIn profile. See, e.g., Maryland State Bar Ass'n, Comm. on Ethics, Ethics Docket No. 2014-06; Philadelphia Bar Ass'n, Prof'l Guidance Comm., Op. 2012-8 (Nov. 2012); South Carolina Ethics Advisory Comm., Op. 09-10; see also note 17.

November 2016



Photo by Chris Ratcliffe/Bloomberg

## Mining Social Data and Putting it to Work

September 2, 2015

**Editor's Note:** *This article is authored by two BakerHostetler partners — an information governance practice leader and a new media, advertising, IT and privacy partner — and an associate.*

By Judy Selby, Alan Friel and Jenna Felz of BakerHostetler

Social media data is a rich source of information for companies competing in today's global marketplace.

Companies can exploit social data for a variety of purposes, such as gaining better knowledge about their customers, improving business intelligence, and developing a competitive edge in the global marketplace. Perhaps the most valuable aspect of "social data" is the variety of data points generated on social media platforms. **Facebook**

(<http://www.businessinsider.com/social-big-data-the-type-of-data-collected-by-social-networks-2-2014-1>) alone collects nearly 60 different pieces of data for its application programming interfaces ("API"), and its "like" button is pressed a staggering 2.7 billion times every day across the web. Facebook users alone post 684,478 pieces of content *per minute*, and Twitter users tweet over 100,000 tweets per minute.

<https://bol.bna.com/mining-social-data-and-putting-it-to-work/>

5/13/2016

The amount of social data being generated is staggering, and many companies are trying to utilize this big data to increase their bottom line. For a technology that is so widely used, however, companies surprisingly have little guidance on the legal implications of collecting and using consumer data generated by social media.

This article is the first in a four-part series. In this article, we provide an overview of the methods by which companies collect social data. In our second article, we will discuss the ways companies analyze social data. In our third and fourth articles, we will identify the legal and ethical considerations companies should keep in mind in collecting, analyzing, and using social data, as well as the risks and challenges posed by the collection and use of social data.

#### The Types of Big Data Collected by Social Media

Social networking sites, chief among them Facebook, Twitter, YouTube, LinkedIn, Google+, and Pinterest, collect a plethora of information about consumers that can be split into two main categories. The first category is information collected about users by the social networking sites themselves, including age, name, sex, gender, interests, occupation, etc. The **second category** (<http://searchenginewatch.com/sew/how-to/2276186/seize-the-data-5-ways-to-leverage-big-data-for-social-media-search>) is information generated by the individual users themselves, including posts, photos, videos, and "like's." Both types of data are available to companies through social network APIs. Companies can create complex, sophisticated algorithms to analyze this data, or use a third party to perform this analysis for a fee.

#### Collecting "Social Data"

Social media platforms use APIs to allow the development of web applications suited to their own programming structure for third parties to use and integrate the platform's service features to their own websites. Through APIs, social media websites can share information seamlessly with companies' apps. APIs allow application developers to access data from social networks in real time. The third party must agree to the platform's terms of use and policies for uploading and publishing information via the API, which limits the ways in which apps can use social data about individual users.

#### *Facebook API*

In 2014, Facebook introduced a new version of its **Facebook Graph API** (<https://developers.facebook.com/docs/graph-api>), which is the primary way to get data in and out of Facebook's social graph. Facebook's social graph is the largest social network data set in the world, and contains the largest number of defined relationships between the largest number of people among all websites. Facebook's social graph is a representation of the information on Facebook, composed of:

- **Nodes** ("things", such as a Facebook User, a photo, a Facebook page, or a comment)
- **Edges** (connections between those "things", such as a Facebook page's photos, or a photo's comments)

- **Fields** (information about those “things”, such as the birthday of a User, or the name of a Facebook page)

To access information contained on Facebook’s social graph, Facebook apps must use the Facebook Graph API. The Facebook Graph API allows Facebook apps to access around 60 different data points, including a User’s Facebook friend list (now restricted to only friends that have connected to the company’s application); a hashtag; a User’s photos on Facebook; Users that “like” a Facebook Page; whether two Users are Facebook friends; the amount of “likes” a Facebook post has; and information about a User’s Facebook profile. It also allows companies to notify existing Users when a User’s friend registers with the app, and allows existing Users to invite their Facebook friends to join the app. For more information on how to use the Facebook Graph API, visit Facebook’s **website** (<https://developers.facebook.com/docs/graph-api>).

#### *Twitter API and Twitter Ads API*

The **Twitter API** (<https://dev.twitter.com/overview/general>) is Twitter’s database of user data that includes every Twitter User’s

personal information, from their age, to who their followers are, and who they follow. It is also the platform that third party apps connect to in order to pull valuable user data to help businesses target their customers more effectively.

There are four main “objects” that the Twitter API tracks: Tweets, Users, Entities, and Places. Users can be anyone or anything. They tweet, follow, create lists, have a home\_timeline, can be mentioned, and can be looked up in bulk. Tweets are the basic atomic building block of all things Twitter. Tweets can be **embedded** (<https://dev.twitter.com/web/embedded-tweets>), **replied to** (<https://dev.twitter.com/rest/reference/post/statuses/update>), **favorited** (<https://dev.twitter.com/rest/reference/post/favorites/create>), **unfavorited** (<https://dev.twitter.com/rest/reference/post/favorites/destroy>) and **deleted** (<https://dev.twitter.com/rest/reference/post/statuses/destroy/%3Aid>). Entities provide metadata and additional contextual information about content posted on Twitter. Entities are never divorced from the content they describe. Places are specific, named locations with corresponding geo coordinates. They can be attached to Tweets by specifying a place\_id when tweeting. Tweets associated with places are not necessarily issued from that location but could also potentially be about that location. Places can be **searched for** (<https://dev.twitter.com/rest/reference/get/geo/search>). Tweets can also be found by the place from which the Tweet was made or is about. For more information on how to use the Facebook Graph API, visit Facebook’s **website** (<https://developers.facebook.com/docs/graph-api>).

The Twitter Ads API was developed in 2013, and allows partners to integrate with the Twitter advertising platform in their own advertising solutions. Selected partners have the ability to create custom tools to manage and execute Twitter Ad campaigns. Twitter’s Advertising API

provides programmatic access to advertising accounts. Partners can integrate their solutions with the API to promote Tweets or Twitter accounts, schedule campaigns, retrieve analytics, manage audiences, and more. To learn more about Twitter's Ads API, visit Twitter's **website** (<https://dev.twitter.com/ads/overview/getting-started>).

These are just two of the many social networking sites that provide valuable information through their APIs. **YouTube** ([https://developers.google.com/youtube/creating\\_monetizable\\_applications](https://developers.google.com/youtube/creating_monetizable_applications)), **Pinterest** (<https://developers.pinterest.com/docs/api/overview/>), **Google +** (<https://developers.google.com/+web/api/rest/>) and **LinkedIn** (<https://developer.linkedin.com/>) also have APIs that can deliver important and timely social data. Companies can also create advanced **algorithms** (<http://snap.stanford.edu/proj/socmedia-www/>) to track the social media information flow in Twitter, which can trace: (1) the spread of a "hashtag" over the network; (2) the spread of a particular URL; and (3) the amount and spread of re-tweets of a company's tweet.

In our next article, we will discuss the ways social data can be analyzed and used by companies to spread brand awareness and increase profits.



## 4 Methods for Analyzing 'Social Data'

September 11, 2015

---

### RELATED CONTENT

---

**Editor's Note:** *This article is authored by two BakerHostetler partners — an information governance practice leader and a new media, advertising, IT and privacy partner — and an associate. It is the second of a four-part series.*

By Judy Selby, Alan Friel and Jenna Felz of BakerHostetler

Our first article (<https://bol.bna.com/mining-social-data-and-putting-it-to-work/>) provided an overview of the methods companies can use to collect data from social media. Once collected, companies can use social data for a variety of purposes, including to: (1) analyze social media interactions, (2) analyze content posted by users, and (3) understand the behavior of specific individuals within a social network, which allows analysis of the characteristics of individuals within social networks and how they are connected to one another.

<https://bol.bna.com/4-methods-for-analyzing-social-data/>

5/13/2016



Social data analysis tools may be used to monitor social networking sites for comments about a company and its products, which entities can use to head off public relations problems and protect the corporate brand. Companies also can measure the effectiveness of their social media strategy in influencing things such as brand recognition and customer sentiment. For example, an organization may collect data about the people following a particular Twitter account — sex, age, location, educational attainment, and even things like annual income or predisposition to purchasing particular kinds of products — which allows companies to create specific, individualized offers to social media users based on this demographic information. Ongoing analysis of uptake on an offer, and comments posted about it, could help the organization refine its message and how it is communicated to improve the response rate and the online feedback.

Some examples of the statistical data that can be collected from social networks and then analyzed include audience distribution, number of impressions for posts, mobile device interactions and responses by users — such as Twitter retweets and click-through numbers for embedded URLs. Content analytics attempt to discern actionable information about the messages that are being posted by the users of social media sites, including monitoring for posts that refer to specific products or brands and tracking customer sentiment based on positive or negative references to a company.

**Four advanced methods (<http://marketingland.com/social-media-advertising-set-explode-next-3-years-121691>) for analyzing social data to target specific audiences are:**

1. Interest targeting: Reach specific audiences by looking at their self-reported interests, activities, skills, pages/users they have engaged with, etc., by searching for particular keywords. Interests can be as general as an industry (e.g. automotive industry) or as specific as a product (e.g. convertibles). Offered by: Facebook, Twitter, LinkedIn (under "Skill"), Pinterest.
2. Behavioral/Connection targeting: With behavioral targeting, companies can reach people based on purchase behaviors or intents and/or device usage. With connection targeting, companies can reach people who have a specific kind of connection to a company's page, app, group, or event. Both types of targeting take past behavior into account to help determine intent. Offered by: Facebook, Twitter, LinkedIn.
3. Custom targeting: Reach audiences by uploading a list of email addresses, phone numbers, users IDs, or usernames. Facebook calls its custom targeting Custom Audiences, while Twitter calls its own Tailored Audiences. Both are largely based on the same concept: if an app has a known group of Users it would like to target, it can simply upload those Users and target them directly (provided that the social network can match the data you're uploading with real profiles). Offered by: Facebook, Twitter.

4. Lookalike targeting: Reach new people who are similar to an audience you care about. Lookalike targeting helps businesses extend their custom audiences to reach new, similar users. For those businesses looking to acquire new customers through social media advertising, lookalike targeting can be a fantastic acquisition tool. Offered by: Facebook, LinkedIn.

The true value in social data is just starting to be realized and monetized – and with the wide proliferation of social media use, is only expected to grow. While social data’s value cannot be argued, companies must keep legal and ethical issues in mind at the outset of any social media project. In our next two articles, we provide tips and strategies for maximizing the value of social data while also complying with legal and ethical obligations and protecting your corporate brand.



Photo by Simon Dawson/Bloomberg

## Best Practices in Collecting and Using Social Data

September 15, 2015

---

### RELATED CONTENT

---

**Editor's Note:** *This article is authored by two BakerHostetler partners — an information governance practice leader and a new media, advertising, IT and privacy partner — and an associate. It is the third of a four-part series.*

By Judy Selby, Alan Friel and Jenna Felz of BakerHostetler

In our first two articles, we discussed the ways in which companies collect, analyze and use data about in connection with social media, which we have termed "social data," for a number of important purposes, such as increasing engagement with their target audience and improving business intelligence. But for all of the potential rewards social data promise, smart companies are thinking in advance about the legal and ethical implications of utilizing social data.

The way organizations choose to collect, use and share data can affect **consumer trust** (<http://pages.altimetergroup.com/The-Trust-Imperative-Report.html>). And establishing an effective and responsible social data framework actually is **demonstrably good for business**

<https://bol.bna.com/best-practices-in-collecting-and-using-social-data/>

5/13/2016

(<http://techcrunch.com/2015/07/17/data-privacy-just-makes-good-business-sense/>).

Before launching into a social data initiative, companies should ensure that their proposed collection and use of social data complies with all relevant legal requirements and is consistent with their consumer's expectations and their corporate brand. Establishing a legal and ethical framework to govern social data projects in advance can help companies avoid missteps and pitfalls, and protect their reputation in the marketplace.

#### *Legal Considerations and Best Practices*

Here are recommendations to help ensure that a company's social data use complies with legal requirements and stays on the right side of consumer expectations.

##### 1. Transparent Privacy Policies

Letting consumers know the types of data to be collected, and the ways that data will be used, is crucial to gaining consumer trust. Providing clear and accurate disclosures as to a company's online services' data practices, and actually complying with these representations to consumers, is required by California law and has been deemed necessary to avoid deceptive or unfair business practices by the Federal Trade Commission. Other countries, such as Canada and EU member nations, have even more consumer protective data privacy laws.

Most companies are aware of this legal framework and have privacy policies posted on their web sites and mobile apps. First, companies should look to see if those privacy representations are limited to data collected via the services on which the policy is posted, or if they are making broader assurances that would include social data collection and use outside of the site or app. Next, even if those policies are restricted to the service on which they are posted, companies need to look at what third party services, including social media plug-ins (e.g., the Facebook "Like" button and tools enabling users to "share" content or activity reporting to third party social media services) and unified sign-in functionality (e.g., using Facebook Connect or Google+ to pull user credentials and other data to sign in on the company's web site), are integrated into the company's service. Integrating third party services into your site or app results in user data being pulled from the social media service to you, as well as pushing user data from your service to the third party social media platform. These practices need to be explained in the service's privacy policy.

Some companies are adding social media functionality to their own sites and apps, allowing users to post or share content and activities on and off of the service. Privacy policies need to explain how this works by default, and what privacy settings or options are available to limit sharing. Privacy policies should also explain how users can change or remove content they have posted (minors in California have certain statutory rights in this regard), and the limitations to changes and removals.

##### 2. Compliance with Third Party Platform Terms

Social networking platforms, chief among them **Facebook** (<https://developers.facebook.com/policy/>) and **Twitter** (<https://dev.twitter.com/overview/terms/agreement-and-policy>), have their own terms of use and privacy policies that explicitly state what information those services collect from users, or permit others to collect from users, and the ways in which that information may be used. This includes limitations on platform users as to how they can collect and use data from the platform. Similar restrictions are included in the licenses platforms grant to other parties that use their code to integrate into the platform, or integrate the platform into their own service. Non-compliance with a social network's terms is a breach of contract and, among other things, may lead the network to terminate an entity's access to the platform.

This was the case with the Sunlight Foundation, a nonprofit organization that works to make government and politics more transparent. It operated a Twitter account called "**Politwoops** (<http://politwoops.sunlightfoundation.com/>)," which preserved and published deleted Tweets of politicians using Twitter's API. On June 3, 2015, Twitter **shut down** (<http://www.cnn.com/2015/06/04/politics/twitter-shuts-down-politwoops/>) Politwoops because preserving deleted Tweets violated its **developer agreement** (<https://dev.twitter.com/overview/terms/agreement-and-policy>). Given the negative consequences that can come with non-compliance, it is very important to ensure that when using a third party platform the use of platform data comply with the platform's rules, and that customers or other parties are not encouraged to engage in practices that would violate the platform's terms and policies.

### 3. Reasonable Data Protection Procedures

Ensuring that reasonable efforts are being taken to maintain the security of collected data should also be a high priority. Companies have a legal duty to provide reasonable security of consumer data in their possession. What is reasonable depends upon the circumstances and the nature of the data. A common error is to make security assurances in a privacy policy, or elsewhere, that are beyond what they company is doing, or even could reasonably be expected to do, which is essentially a false or deceptive claim. The **FTC** (<https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises>) and many states' attorneys general, chief among them **California** (<https://oag.ca.gov/privacy/privacy-enforcement-actions>), have targeted companies for failing to abide by their privacy policies and/or maintain adequate data security protocols. Of course, it is impossible to guarantee data security will not be compromised, so companies should have a breach preparedness plan, especially if they have data covered by state breach notification laws.

### 4. Compliance with Legal and Self-Regulatory Restrictions

Companies using social media in marketing campaigns should also be aware of the legal implications of doing so. Just because a user has publicly posted content, or their activity has been publicly reported on a social media platform of which they are a member, does not mean that a company can necessarily re-distribute or make other use of that data. The user has granted permission to the social media platform, and that platform's terms of use will determine the extent to which third parties, including others on the platform, may use the content and data.

For instance, while a platform may obtain the right from users to let other users re-post or otherwise use user-posted content on the platform, most do not obtain the rights from users, or grant users the right to remove platform content and post it in other places such as on a company's own web site or in its off-platform advertising, marketing and promotion. Such uses should be cleared by getting permission from the user who posted the content. Otherwise, a company may face copyright infringement, rights of publicity and false endorsement claims.

Using a platform API feed to display platform content in a window on a Company's own site, as opposed to cherry picking posts and republishing them, may or may not be authorized depending upon the platform's terms of use and developer and API terms. Even on-platform use may not be authorized. Facebook, for instance, has settled class actions by users who claimed that Facebook's then current terms of use did not obtain user consent to associate them with Facebook advertisers when they "liked" a brand, and by notifying the user's friend's that the user liked the brand, Facebook and the brands were making a false endorsement and violating the user's rights of publicity. Facebook has since revised its terms to make the consent to do so more clearly and also added privacy controls that let users limit how their likes are conveyed to others.

Companies that serve or advertise to children should be particularly careful with social media including integrating social media plug-ins on their own web sites. The **Children's Online Privacy Protection Act** (<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>) restricts collection, use and sharing of certain data (including IP address, unique identifiers, geolocation data, pictures and name and contact information) of children under 13 absent verified parental consent or narrow exceptions. This makes most social media features and functionality out-of-bounds for children.

Social data is valuable for enabling targeted advertising, since the advertiser can limit ads to consumers that fit a profile suggesting they would be interested in the product or service advertised. When these profiles are gathered based on user activities across sites and services, there are legal and self-regulatory requirements that may apply. California law requires web sites and mobile apps to include certain disclosures in their privacy policies when they engage in such activities, or permit others to do so in connection with their service. The

U.S. advertising and publishing industries have developed a notice and opt-out program for interest-based ads based on user profiles developed from collecting data about their activities across time and services. For more information see [www.aboutads.info](http://www.aboutads.info)

5. Social Data Record Retention

Companies facing the threat of potential future litigation or regulatory investigation should retain data collected from social media services for a reasonable period of time. Data collectors may face harsh penalties for spoliation of electronic records evidence, as recent case law has raised the bar for maintenance and production of electronic files such as databases, and emails in anticipation of and during litigation. It is therefore important to implement comprehensive record retention policies and procedures with respect to data collected from social media to the extent it may be relevant to the threatened litigation or government investigation.

6. Consider Privacy and Security Early and Reassess Practices Regularly

As social media evolves, as technology increases, as the company gains more experience and its comfort level grows its social media data practices will change. By instituting privacy-by-design and security-by-design into the development process privacy and security impacts can be identified and mitigated as a practice, campaign or product is being designed, rather than as an afterthought when it may be too costly or time consuming to make changes. Also, given that social media, and thus how you use it, is evolving, companies should reassess practices regularly and determine if they need update its policies and procedures.

In our fourth and final article in this series, we will discuss ethical considerations in the collection, analysis, and use of social data.

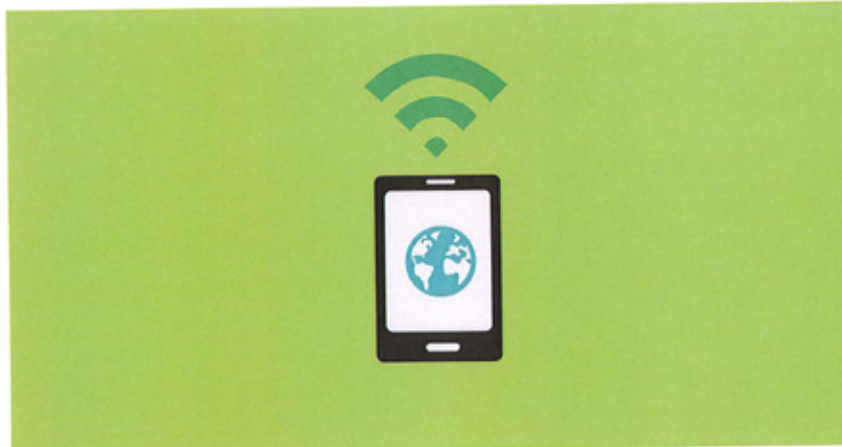


Illustration by Joe The Goat Farmer (Flickr/Creative Commons)

## Ethical Considerations in Using Social Data

September 22, 2015

---

### RELATED CONTENT

---

**Editor's Note:** *This article is authored by two BakerHostetler partners — an information governance practice leader and a new media, advertising, IT and privacy partner — and an associate. It is the final of a four-part series.*

By Judy Selby, Alan Friel and Jenna Felz of BakerHostetler

In our last article, we discussed the legal considerations in collecting, analyzing, and using social data. Complying with the black letter of the law is critical, but not enough; companies need to consider how their contemplated use of social data will be perceived by their customers and in the marketplace as a whole.

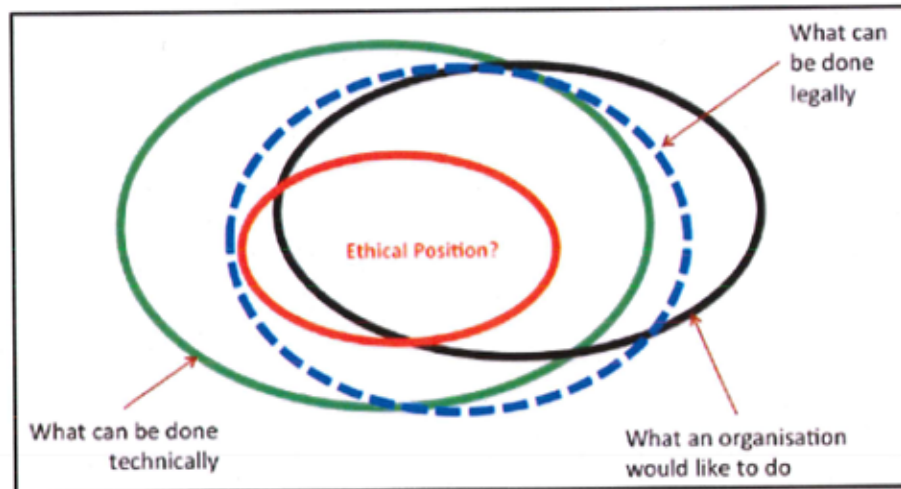
Companies should ask themselves, will the use of social data be viewed as intrusive, exploitative, or "creepy?" And is the use consistent with the image the company wants to project, particularly to its consumer base and investors?

"The complexity and, at times, intimacy, of social data opens up many unexplored ethical questions that when left unaddressed can lead to reputational and legal risk," said Susan Etlinger, industry analyst at Altimeter Group, a research and advisory firm. "Organizations that



accept this reality now, and expand their governance frameworks to address social data, will be better positioned to retain the trust and loyalty of their constituencies — even as new technologies emerge.”

The IBM UK and Ireland Technical Consultancy Group (TCG) created an “ethical awareness framework” to help businesses develop ethical policies for their use of analytics and big data.



*Photo Credit: UK and Ireland Technical Consultancy Group (TCG)*

(<https://bol.bna.com/wp-content/uploads/2015/09/Ethical.png>)

According to the framework, businesses should consider the wider implications of their activities when collecting, using, and storing data, including:

- Context – For what purpose was the data originally surrendered? For what purpose is the data now being used? How far removed from the original context is its new use? Is this appropriate?
- Consent & Choice – What are the choices given to an affected party? Do they know they are making a choice? Do they really understand what they are agreeing to? Do they really have an opportunity to decline? What alternatives are offered?
- Reasonable – Is the depth and breadth of the data used and the relationships derived reasonable for the application it is used for?
- Substantiated – Are the sources of data used appropriate, authoritative, complete and timely for the application?
- Owned – Who owns the resulting insight? What are their responsibilities towards it in terms of its protection and the obligation to act?

- Fair – How equitable are the results of the application to all parties? Is everyone properly compensated?
- Considered – What are the consequences of the data collection and analysis?
- Access – What access to data is given to the data subject?
- Accountable – How are mistakes and unintended consequences detected and repaired? Can the interested parties check the results that affect them?

These issues are important for all companies that use data, but they are particularly important for companies with business plans that depend on consumers, customers, or clients being willing to entrust their data to the business. As data collection methods evolve, the amount of data collected by companies will grow, and data security concerns will rise. As a result, a company's reputation and consumer trust will increasingly become of paramount concern. Implementing best practices now, and continuously revising them as the company and the technology grow and change, can make the all the difference in the eyes of the law and the public.