

Corporate Legal Ethics
Presented by ISBA Corporate Law Departments
Section

Social Networking: An Ethical Issues
Update

Gregory G. Thiess
Vice President and Assistant General Counsel
Robert Bosch LLC

Topics

- **Trends - Use of Social Media in the Workplace and Use of Social Media in General**
- **Compliance - Fair Credit Reporting Act and FTC Enforcement Guidelines**
- **Compliance – OFCCP Enforcement and EEOC Requirements**
- **Accuracy, Reliability and Usefulness of Social Media Data**
- **Public Policy Violations - Adverse Employment Issues for Off-Duty Conduct**
- **Employer Access to Employee Social Media Pages**
- **Protection of Company Confidential, Trade Secret and Proprietary Data**
- **National Labor Relations Board Oversight - Employee Posts in Social Media as Concerted/Protected Speech**
- **Federal Trade Commission Oversight - Updated “.com Disclosure” Guidelines and Endorsements**
- **Ownership of Social Media/Connections Developed by Employees**
- **Employee Claims - Discrimination/Defamation and Related Lawsuits**
- **Claims By Companies - Defamation, Interference With Business**

Trends

Use of Social Media in the Workplace

Background – Use of Social Media by Employers/Employees

- An increase (<10% in 2012 to 60% in 2015) in employer monitoring of worker social media use, to detect security breaches, is expected.¹
- 92% of U.S. employers admit they use or plan to use social media to assess job candidates (10% increase over 2010), and 73% report they successfully hired at least one person found on social media.²
- 86% of recruiters report that they will look at applicant social profiles (48% always, 25% occasionally and 13% if provided).³
- References to use of illegal drugs (78%), posts of a sexual nature (66%), use of profanity (61%), spelling/grammar errors (54%) and pictures of alcohol consumption (47%) were viewed as negatives by recruiters.⁴
- Memberships in professional organizations (80%) and volunteering or donating to charities (66%) are viewed as positives by the recruiters.⁵
- Political posts (62%) and “overtly” religious posts (53%) viewed as neutral.⁶

Background – Survey of Social Media Use in the Workplace

“Most companies allow some type of access to social media at work.”

- 43% of respondents work in organizations with open social media access.
- 24% of respondents work in organizations where access is monitored.
- 16% said access to social media was completely blocked.

“Virtually no employers are asking for social media passwords.”

- Despite media/political interest, 97% of respondents say their employer or potential employer had not asked for social media passwords.

“Employees use mobile devices frequently during working hours to access personal social media.”

- 60% of respondents check personal social media more than once /day on their mobile devices; 3 out of 4 workers check once a day or more.

“Interacting with co-workers was the primary motivator for social media engagement during the workday.”

- 49% say connecting with co-workers is top reason to use social media at work.
- Next most popular reasons are connecting with others on a fun social platform (47%) and connecting with customers (44%).”⁷

Background – Survey of Social Media Use in the Workplace

“Twitter is overwhelmingly the most popular social media site accessed at work.”

- 70% of respondents use Twitter, 65% use Facebook, 19% use corporate intranets.

“Companies’ efforts to guide employee use of social technology are mixed.”

- 23% of respondents report having a specific social media policy from their employers.
- 23% of respondents report having no policy at all.
- 17% of respondents said their employers had issued informal guidelines.
- Less than 10% of employers offer social media training to employees.

“When it comes to interacting with customers through social platforms, marketers lead and customer service is surprisingly behind.”

- Of employees who use social media to connect with customers, 26% are in marketing.
- Customer support (3.1%) and product management (2.9%) reported modest use of social media to contact customers.”⁸

Trends

Use of Social Media in General

Background – Use of Social Media in General

- Facebook has over 1.2B active users, up from 845M one year ago, with an average user time per month of 15 hours, 33 minutes and 70B pieces of content shared each month.⁹
- Twitter is now one of the top 10 most visited social media sites, with over 500M active users (up from 100M one year ago), and an average of 8,900 new tweets/second and 1.6B search engine queries/day.¹⁰
- YouTube now receives an average of 60 hours of uploaded video every minute (versus 48 hours/minute one year ago), and reports 800M unique visits/month and 4B videos viewed/day.¹¹
- LinkedIn now has over 200M members and 2.7M companies with LinkedIn pages, and its site had over 5.7B professionally oriented searches in 2012.¹²
- Flickr has 75M users, with 3K new photos posted per minute.¹³

Compliance

**Fair Credit Reporting Act (FCRA), 15 U.S.C. §
1681 et seq.**

**Federal Trade Commission FCRA Enforcement
Guidelines**

Compliance With Fair Credit Reporting Act

“Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA”¹⁴ (June 12, 2012).

Spokeo, Inc., a data broker that compiles and sells detailed information profiles on millions of consumers, will pay \$800,000 to settle Federal Trade Commission charges that it marketed the profiles to companies in the human resources, background screening, and recruiting industries without taking steps to protect consumers required under the Fair Credit Reporting Act.”

- First Commission case to address sale of Internet/social media data for employment screening.
- FTC alleged that Spokeo operated as consumer reporting agency and violated FCRA by:
 - Failing to assure that information it sold is used only for legally permissible purposes.
 - Failing to assure that information it sold was accurate.
 - Failing to tell users of its reports about their FCRA obligations to notify consumers if the user took an adverse action against the consumer based on information in the consumer report.
- FTC also claimed Spokeo posted misleading on-line endorsements of its service, which suggested that the endorsements were independent when in fact they were posted by Spokeo's employees.
- FTC said case is part of its “ongoing enforcement of the FCRA, a law passed by Congress to promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies, and to regulate the use and dissemination of consumer reports”.

Compliance With Fair Credit Reporting Act – Lawsuits

Hinton v. Universal Background Screening, 12-cv-01355 (E.D. Pa. filed March 15, 2012, settled Dec. 20, 2012).

- Alleged FCRA violation when consumer reporting agency reported a misdemeanor conviction as a felony and failed to provide notice of finding to Plaintiff, resulting in denial of employment.

Darlene Martinez v. Universal Background Screening, 12-cv-02183 (D. AZ Oct. 11, 2012), pending.

- Alleges FCRA violation when Universal twice reported felony convictions of a person named on Plaintiff's report, which were actually convictions of a "Darlene Ramirez".
- Failed to provide notice of finding to Plaintiff, resulting in denial of employment.

In the Matter of Filiquarian Publishing, LLC, et. al., FTC File No. 112 3195.

- FP sold mobile apps allowing buyers to conduct criminal background checks, but disclaimed that it was FCRA compliant, said its product was not for employment, insurance or credit screening, and that buyers assumed responsibility for FCRA compliance.
- Complaint alleges FP violated FCRA by:
 - providing consumer reports without a process assuring they were for FCRA allowed purposes.
 - providing reports without procedures to assure accuracy.
 - not providing required credit reporting agency notices to app users.
- On Jan. 10, 2013, FP agreed to 20 year Consent Order with steps to assure regulatory compliance and requirements for regular compliance reporting to FTC.

Compliance With Fair Credit Reporting Act – Employer Obligations

- **“Using Consumer Reports: What Employers Need to Know”** ¹⁵
 - **Before Employer Obtains Consumer Report:**
 - Tell applicant/employee, in writing, you may use information in report for employment decisions.
 - Notice must be a stand-alone writing and cannot be in an employment application.
 - Must obtain written permission from applicant /employee.
 - Certify to companies from which you get applicant/employee information that you:
 - Notified applicant or employee and got their permission to get a report.
 - Complied with FCRA requirements.
 - Will not discriminate or use information against them contrary to equal employment opportunity laws.

- **Before Employer Takes Adverse Employment Action, you must give applicant/employee:**
 - Notice, including a copy of the report you relied on to make the decision.
 - Copy of FTC’s “A Summary of Your Rights Under the Fair Credit Reporting Act”.

- **After You Take an Adverse Action Based on Information in a Consumer Report, you must:**
 - Give applicant/employee notice of adverse action, orally, in writing or electronically, including:
 - Name, address and phone number of the consumer reporting company supplying the report.
 - Statement that reporting agency did not make the adverse decision and can’t give specific reasons for it.
 - Notice of right to dispute accuracy of report, and to get additional free report if requested within 60 days.

- **Disposing of Consumer Reports**
 - When done with the report, you must securely dispose of it and any information taken from it.
 - May include “burning, pulverizing, or shredding paper documents and disposing of electronic information so that it can’t be read or reconstructed”.

Compliance

**Office of Federal Contract Compliance
(Executive Order 11246)**

and

EEOC Requirements

Possible Access to and Misuse of Data – Discrimination Claims

→ OFCCP News Release: Baldor Electric to pay \$2 million to settle hiring discrimination case with US Labor Department

WASHINGTON – The “Office of Federal Contract Compliance Programs today announced that Baldor Electric Co. has agreed to settle allegations of systemic discrimination stemming from the company's applicant screening process at its facility in Fort Smith, Ark. OFCCP investigators determined that the process violated Executive Order 11246 by creating a disparate impact on women and minorities. As a result, 795 qualified women, African-Americans and job seekers of Asian and Hispanic descent were denied the opportunity to advance to the interview stage when applying for production and laborer positions.”¹⁶

- OFCCP Investigation focused on applicant background check process, which agency claimed used illegal criteria to eliminate minority applicants from job interview process. As a result of settlement, Baldor will:
 - Pay \$2M in back wages/interest to affected individuals and make at least 50 job offers to members of class.
 - Implement self-monitoring steps to assure hiring processes meet OFCCP laws and record-keeping requirements.

→ EEOC v. Pepsi Bottling Group (EEOC Jan. 11, 2012).

- Allegation that criminal background checks conducted, but company used results of arrests without conviction and convictions of minor offenses to exclude applicants.
- Effect alleged to be a disproportionate effect on African-American applicants.
- Settlement of \$3.13M, job offers to some affected applicants and changes in its background check policies.

Possible Access to and Misuse of Data – Discrimination Claims

- **New OFCCP Directive “Complying with Nondiscrimination Provisions: Criminal Record Restrictions and Discrimination Based on Race and National Origin”.**¹⁷
- Notes that in recent decades “the number of Americans who have had contact with criminal justice system” has increased “exponentially” and that disproportionate number and percent of such persons are minorities.
 - “In light of these racial and ethnic disparities, contractors should be mindful of federal anti-discrimination laws if they choose to rely on job applicants' criminal history records for purposes of employment decisions. Hiring policies and practices that exclude workers with criminal records may run afoul of such laws... . Due to racial and ethnic disparities in the criminal justice system, such policies are likely to violate federal anti-discrimination law.”
 - Directive also cites EEOC/FCRA enforcement policies, and Work Opportunity Tax Credit for employers hiring felons.
 - Directive available at <http://www.dol.gov/ofccp/regs/compliance/directives/dir306.htm>.

Accuracy, Reliability and Usefulness of Social Media Data

Accuracy, Reliability and Usefulness of Social Media Data – Business Use

- **“Big Data: Businesses Wary of Analytics based on Unknown Social Media Data Quality.”**¹⁸
- Report from IBM and Oxford business school found two-thirds of companies think “Big Data” can be useful, but ... “70 percent of them are only in the very early stages of evaluation of the technology”.
 - “In particular, data collected from Social Media outlets is suspect At this point, only 39 percent of those surveyed said that they collect any social data, and only 7 percent said that social-media derived data plays an important part of their data analysis. While a top reason many businesses pursue Big Data projects is to be able to improve their customer service/experience, many are wary that data derived from social media is accurate.”
 - “Garbage in — Garbage out. It’s a major problem with any data analysis. ... [O]nce the data is captured, how accurate is it and can any analysis based on it truly be trusted? Data cleansing is a process that’s difficult to do well even with a data set that’s been generated internally and is well understood. It’s a much more difficult question to quantify data quality when dealing with data that originated from external sources.
 - “One key reason for companies not collecting and analyzing wider varieties of data lies in the veracity – or truthfulness – of insights generated from sources such as real-time data and social media. Striving for high data quality is an important Big Data requirement, and the survey respondents questioned the ability to trust rapidly growing forms of unstructured data, such as those generated from on-line consumer comments, reviews, Tweets and other forms of freely offered opinions.”

Public Policy Violations

Adverse Employment Issues for Off-Duty Conduct

Public Policy Violations – Adverse Employment Issues for Off Duty Conduct

- At present, 29 states and the District of Columbia have laws protecting employees from adverse employment actions based on off-duty behavior.¹⁹
 - 18 have "tobacco only" statutes.
 - Connecticut, District of Columbia, Indiana, Kentucky, Louisiana, Maine, Mississippi, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Virginia, West Virginia, and Wyoming.
 - 8 states protect the use of lawful products.
 - Illinois, Minnesota, Missouri, Montana, Nevada, North Carolina, Tennessee, Wisconsin.
 - 4 states protect employees who engage in lawful activities.
 - California, Colorado, New York, and North Dakota.

Employer Access to Employee Social Media Pages

Employer Access to Employee Social Media Pages

→ **Six states outlaw employer snooping on Facebook.**²⁰

Six states have now made it illegal for employers to ask applicants/employees for passwords or access to private portions of their social media accounts.

- California
- Illinois
- Michigan
- New Jersey
- Maryland
- Delaware

→ For a current summary of the new statutes in these states, and legislative efforts similar to them in Massachusetts, Minnesota, Missouri, New York, Ohio, Pennsylvania, S. Carolina and Washington, see “Employer Access to Social Media Usernames and Passwords - 2012 Legislation - Year-end summary (Jan. 17, 2013)”, published by the National Conference of State Legislatures, at <http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx>.

Protection of Company Confidential, Trade Secret and Proprietary Data

Protection of Company Confidential, Trade Secret and Proprietary Data - Issues

- Employees with access to company confidential, trade secret or proprietary data can compromise its confidential character by sharing it through social media postings or discussions with social media contacts.
- Data may become accessible to competitors, opponents in litigation or others who have no rights to see it or whose access to the data is properly conditioned on NDA or protective order.
- Company efforts to protect against such disclosures of confidential data, if not carefully drawn, may violate rights governing protected speech of employees.
- Disclosures on social media of information deemed to be company disclosures subject to securities regulations.
- Employee use of social media to access confidential, trade secret or proprietary data of competitors or others that company has no right to see.

Protection of Company Confidential, Trade Secret and Proprietary Data – Steps to Protect²¹

1. Identify information your business considers trade secret, proprietary or otherwise confidential.
2. Insure that such confidential information is marked as such and that employees have written notice of its status.
3. Execute policies and procedures to limit access to such confidential information.
4. Implement procedures that limit electronic access, transmittal or downloading of such information.
5. Execute policies informing employees that information they obtain during their employment belongs to employer.
6. Maintain confidential information and documents in company accessible databases or files only and do not allow employees to keep it in personal files.
7. Have employees execute agreements acknowledging/agreeing that company owns the confidential documents.
8. Develop and publish social media policies, to provide direction to employees regarding appropriate use of social media without violating NLRA protections for protected and concerted activities.
9. Social media policies should also include agreements that company owns social media accounts developed/used by employees to promote the company's business, and access and passwords to such social media accounts.
10. Require confidential information to be collected from employees leaving company or transferring to other positions in the company where access to the information is not required.
11. Collect computers and other personal devices from departing employees and, if needed, inspect them for misuse.
12. Develop procedures to return computers, database access and network devices, and access/passwords for each.

National Labor Relations Board Oversight

Employee Posts in Social Media as Concerted and

Protected Speech

Employee Posts in Social Media as Concerted and Protected Speech

- NLRB has aggressively reviewed and filed cases against employers that discipline employees for making on-line negative posts about their employers and supervisors, if the agency believes that the discipline is contrary to NLRA protections for concerted and protected activity under Section 7 of the NLRA.
- NLRB Memoranda issued August 18, 2011²² and January 24, 2012²³ by NLRB Acting General Counsel Lafe Solomon, outlining 28 cases the agency investigated in 2010 – 2011, involving employee use of social media and employers' social and general media policies.
- NLRB has since issued, on May 30, 2012,²⁴ a third memo focusing on the legality of employer policies attempting to control employee use of social media, and potentially discipline employees for violations of such policies.
- Six of the seven policies examined in the memo were determined to be illegal in one or more respects because, in the NLRB's view, the policies impermissibly restricted the exercise by employees of their Section 7 rights.
- The text of the one policy found to be entirely legal in the third NLRB memo, a Walmart "Social Media Policy" implemented May 2012, is attached to this presentation as Exhibit 1 and should be used by policy drafters as guidance.

Employee Posts in Social Media as Protected Speech

- **Third NLRB memo signals that employer social media policies will be carefully reviewed by the agency to determine if, in NLRB's view, they restrict employee exercise of Sec. 7 rights.**
- Policy drafters should consider the following when drafting social media policies:
 - Posting disparaging comments that do not discuss wages, hours, other terms or conditions of employment, or that do not include other employees are likely not protected Sec. 7 activities.
 - Postings that are simply “egregious and offensive” may not be protected activities.
 - Policies may prohibit “commercial use” by employees of company assets (e.g. TMs, company logos).
 - Policies may restrict employees from using social media during work hours or with company devices.
 - Policies should include specific examples of prohibited or restricted behavior, so that employees can distinguish what is prohibited from what is protected activity.
 - “Savings clauses” (e.g. “Nothing in this policy should be construed to limit employee rights under the NLRA”) are recommended, but will not save a policy that otherwise restricts Sec. 7 rights.
 - “Courtesy clauses” can be used to promote civil behavior, but may be illegal if they restrict Sec. 7 activities.
 - Opinions stated by employees while engaged in Sec. 7 activities, even if incorrect, should not be prohibited.
 - Policy restrictions on employees giving third party interviews will likely be found to violate Sec. 7.

Federal Trade Commission Oversight
Updated “.com Disclosure” Guidelines

Federal Trade Commission Oversight - Updated “.com Disclosure” Guidelines

“FTC's Updated .com Disclosures Guidance”²⁵

- “The Federal Trade Commission (“FTC”) issued new guidance for digital advertisers and marketers, “.com Disclosures: How to Make Effective Disclosures in Digital Advertising” on March 12, 2013. The guidance is designed to help mobile and other online advertisers make disclosures clear and conspicuous to avoid deception.

The revision to the Dot Com Disclosures Guide is the first since 2000, when smart phones, tablets, and social media marketing were not in wide use. The revised Guide emphasizes that consumer protection laws apply equally to marketers across all mediums, whether delivered on a desktop computer, a mobile device, or more traditional media such as television, radio, or print.”

- New .com Disclosures Guidance at: <http://www.business.ftc.gov/legal-resources/com-disclosures-how-make-effective-disclosures-digital-advertising-march-2013>.

Federal Trade Commission Oversight - Updated “.com Disclosure” Guidelines

FTC Reboots .com Disclosures: Four Key Points, One Possible Way to Bypass the Issue Altogether²⁶

- “.com Disclosures focuses on the same consumer protection principles, but fast-forwards them to reflect changes in the digital marketplace. Here it is, distilled down to four key points:”
- “The most important thing about the new .com Disclosures is what hasn’t changed. Regardless of how or where you market, well-established truth-in-advertising principles apply.”
- “[I]f the disclosure of information is [n]ecessary to prevent an online ad claim from being deceptive or unfair, it has to be clear and conspicuous. So what’s new? According to .com Disclosures ..., advertisers should make sure their disclosures are clear and conspicuous on all devices and platforms that consumers may use to view their ads.”
- “The old guidelines defined “proximity” as “near, and when possible, on the same screen.” The new advice: Disclosures should be “as close as possible” to the relevant claim. Another design consideration ... was ... to avoid buried or generically labeled hyperlinks [or] ... using hyperlinks for disclosures involving key information” (e.g. cost or safety information). “The new document ... call[s] on advertisers to label hyperlinks as specifically as possible.”
- “One big development since 2000: space constraints in ads, including on social media platforms. The new .com Disclosures acknowledges the challenge ..., but companies still have to make necessary disclosures clearly and conspicuously. Disclose via pop-ups? “Not a good idea since there are so many technologies for blocking them.”
- FTC “Bypass”? “Rather than focusing on fonts, hyperlinks, proximity, platforms, and the whole disclosures rigamarole, how about stepping back and reformulating the ad claim to get rid of the need for disclosure?”

Federal Trade Commission Oversight

Endorsements

Federal Trade Commission Oversight - Endorsements

Paying for endorsements of company services, products or accomplishments may create claims of deceptive trade practices or false statements.

- **Are your product/service/company claims based on real social media data?**
- **“Gartner Says By 2014, 10-15 Percent of Social Media Reviews to Be Fake, Paid for By Companies”²⁷**
- “Consumers’ increased reliance on social media ratings and reviews will see enterprise spending on paid social media ratings and reviews increase, making up 10 to 15 percent of all reviews by 2014, according to Gartner, Inc. However, analysts predict that increased media attention on fake social media ratings and reviews will result in at least two Fortune 500 brands facing litigation from the U.S. Federal Trade Commission (FTC) over the next two years.

...

Many marketers have turned to paying for positive reviews with cash, coupons and promotions including additional hits on YouTube videos in order to pique site visitors' interests in the hope of increasing sales, customer loyalty and customer advocacy through social media ‘word of mouth’ campaigns.

...

Marketing, customer service and IT social media managers looking to use reviews, fans and ‘likes’ to improve their brand's reputation on social media must beware of the potential negative consequences on corporate reputation and profitability” ... CMOs will need to weigh the longer-term risks of being caught and the associated fines and damage to reputation and balance them against the short-term potential rewards of increased business and the prevailing common business practice in their market, often regardless of ethics.”

Federal Trade Commission Oversight - Endorsements

“Endorsement-based Advertising Subject to Law Enforcement by FTC”²⁸

- “In some cases, user endorsements leverage social media features. For example, a company's website may include a button that, when clicked by a user, causes a positive message about the company to be posted via the user's Facebook, LinkedIn, Twitter, or other social media account. When there is compensation for that endorsement--even soft compensation such as through loyalty program points or virtual goods--federal laws may come into play.”
- The endorsement guidelines impose requirements on both the endorser and the advertiser if there is a "material connection" between the two parties.
- A material connection may arise when an endorser is compensated for the endorsement, for example, by payment, free samples, coupons, or other benefits.
- If there is a material connection it must be "clearly and conspicuously" disclosed. The advertiser also has a duty to notify endorsers about the disclosure requirement and advertisers must have procedures in place to monitor endorser compliance.
- Although both endorser and advertiser are subject to these requirements, FTC has indicated that its enforcement will focus primarily on advertisers.

Ownership of Social Media/Connections

Developed by Employees

Ownership of Social Media/Connections Developed by Employees

PhoneDog v. Kravitz, U.S. District Court, ND Cal., C11-03474, filed 07/15/2011.

- PhoneDog hired Kravitz to write product reviews and post/link blog entries to generate traffic to PhoneDog web page. Also gave Kravitz password and Twitter handle “@PhoneDog_Noah.” Kravitz efforts generated 17,000 Twitter followers, which PhoneDog claimed had a value of \$2.50/Twitter follower per month (\$42,500/month).
- When Kravitz left PhoneDog in late 2010, PhoneDog requested Kravitz turn over control of the account – Kravitz refused and continued to use it under “@noahkravitz”.
- PhoneDog sued claiming (i) misappropriation of trade secrets; (ii) intentional and negligent interference with prospective economic advantage; and (iii) conversion.
- Case settled in December 2012 (with District Court retaining jurisdiction to assure enforcement), but Kravitz allowed to keep the Twitter account and followers while changing account name to “@noahkravitz”.

Eagle v. Morgan, et al., U.S. District Court, ED PA, 11-cv-04303, filed 07/01/2011.

- Suit filed by founder/former President of “Edcomm” against later purchasers over ownership and control of the Eagle’s LinkedIn account and its “connections” to other LinkedIn members.
- After company terminated Eagle it changed Eagle’s profile to display the photo and profile of Eagle’s replacement. Eagle sued claiming invasion of privacy and tortious interference. Edcomm counterclaimed, alleging misappropriation of LinkedIn account and unfair competition.
- In Oct. 2012 Court dismissed Eagle’s federal claims but ordered case to proceed on Eagle’s state law claims and Edcomm’s counterclaims for misappropriation of the LinkedIn account and unfair competition.
- On Dec. 31, 2012, Court ruled for Edcomm, dismissed Eagle’s state claims, awarded Edcomm damages of \$41k and enjoined Eagle from accessing or using the LinkedIn account. Post-trial motions pending.

Ownership of Social Media/Connections Developed by Employees

Ardis Health v. Nankivell, et.al., U.S. District Court, SD New York, 11-cv-05013, filed July 2011.

- Employer suit against former employee alleging employee refused to return a laptop/work equipment, and passwords/login information for work-related websites, email/social media accounts and third party servers.
- When hired, employee signed agreement providing that work he created is “exclusive property of [Employer], in whatever stage of development” and that it is a “work-for-hire” within meaning of Copyright Act of 1976.
- Former employee counterclaimed saying she owned the social media web site she created while working for Ardis, that Ardis destroyed certain of her private property and that she was subjected to hostile work setting.
- In Oct. 2011 Court ordered employee, based on employer-employee agreement, to return passwords/login information, and in Oct. 2012 dismissed employee counterclaims (some for lack of jurisdiction, others on merit).

Cases appear to be holding that:

1. Employer/employee agreements governing ownership rights of employee developed social media sites, access and log-in data, content and identities of followers/users are enforceable.
2. Absent explicit agreement covering ownership rights of social media sites and information, Courts will examine the extent of employer’s contribution to creating the site when determining questions of post-employment ownership.
3. The fact that employee accessed employer data files when creating a social media site may not be a significant factor in determining ownership, if employee properly had access to such files when employee created the site.

Employee Claims

Discrimination/Defamation and Related Lawsuits

Claims By Employees – Defamation, Discrimination

- **Cockram v. Genesco, Inc.**, 680 F. 3d 1046 (8th Cir. 2012).
 - Plaintiff appealed dismissal of suit against former employer for defamation and false light invasion of privacy.
 - Plaintiff fired for allegedly adding a racial slur to a return receipt she printed, signed and gave to a customer.
 - Press coverage of the incident included Genesco statement that it was “shocked and sickened” by incident and that the employee was fired. Plaintiff alleged news coverage led to accusations of racism and threats.
 - Next day Genesco found that another former employee programmed the slur into the system Plaintiff used to issue receipt. Slur was tied to a generic phone number Plaintiff used to enter return into Genesco system.
 - Genesco issued a clarifying statement, but did not absolve Plaintiff, in part because Plaintiff violated company policy by using generic phone number to enter return. Genesco asserted its statements were true.
 - Court reversed dismissal of Plaintiff’s defamation claim, finding that a jury could “conclude that Genesco’s statements were false, that they harmed Cockram’s reputation, and that this harm was distinguishable from any harm flowing from the generic news stories” of the event.

- **TerVeer v. Billington (Librarian of Congress)**, Civ. Action 12-1290, USDC DC., filed August 3, 2012 (pending).
 - Claim of sex stereotyping, gender, religious discrimination, retaliation, violations of Library of Congress statutes and regulations, following discovery by Plaintiff’s supervisor that Plaintiff was homosexual.
 - Discovery of Plaintiff’s sexual orientation came from supervisor’s daughter, who saw on Plaintiff’s Facebook page that Plaintiff had “liked” certain web sites supporting same sex parents.
 - Daughter asked if Plaintiff was homosexual. When Plaintiff said yes, daughter ended Facebook connection.
 - Plaintiff alleges that after disclosing his sexual orientation to supervisor’s daughter, his work environment was made hostile by his supervisor, ultimately leading to his termination.

Claims By Employees – Defamation, Discrimination

- **Espinoza v. County of Orange, CA**, No. G043067, Unpub. Opinion, Ct. of Appeals CA, 4th Dist., Feb. 9, 2012.
 - Claim of workplace harassment of Plaintiff (physically disabled person), in part through an on-line blog created by a co-employee on his personal computer.
 - After learning of blog, County took steps to determine who was using County computers to access blog and to limit, but not prohibit, blog access. Access to blog blocked ~2 months later.
 - County identified employees accessing blog, but never interviewed or disciplined them. Plaintiff went on disability, alleging illnesses arising from the harassment.
 - Jury returned Plaintiff verdict of \$820K (lost earnings, mental distress). Trial court awarded \$194K fees.
 - On appeal, County claimed it could not be held liable because:
 - Blog postings were anonymous and not made by County.
 - County did not create or approve the blog.
 - Verdict violated 1st Amendment freedom of speech, and is preempted by Communications Decency Act.
 - Verdict not supported by evidence sufficient to prove CA Fair Employment and Housing Act claims.
 - Judgment for Plaintiff affirmed. Not appealed to Cal. Supreme Court.

- **Armstrong v. Shirvell**, Civ. Action 11-cv-11921, USDC ED MI., May 2, 2011 (Post-trial motions pending).
 - Claim of defamation, emotional distress, abuse of process, invasion of privacy, stalking (President of Student Assembly at U. Mich.), through Facebook group developed by Defendant and a self-generated blog.
 - Allegations on Facebook and in blog included, among others, claims about Plaintiff's sexual orientation, racial views, religious beliefs, that Plaintiff supported violence, that Plaintiff was a Nazi, etc.
 - Much of the claimed abuse occurred while Defendant was a Michigan Assistant Attorney General.
 - Case went to trial in August 2012, and a verdict was returned for Plaintiff on all counts, totaling \$4.5M.

Claims By Companies

Defamation, Interference With Business

Claims By Companies – Defamation, Interference With Business

- **Clay Corp. v. Colter**, CV-12-01138, Mass. Super. Court, Norfolk County, Sept. 12, 2012).
 - Claim of defamation/interference with customer relations by car dealer against former employee's relatives who began "Boycott Clay Nissan" Facebook page and social media campaign against Clay after sister fired.
 - Defendants' social media campaign alleged sister was terminated "because she had cancer".
 - Dealer sought injunction, damages and attachment of defendants' assets pending outcome of case.
 - Trial court ordered \$1.5m attachment against defendant assets, based on preliminary determination of likely success by Plaintiff and risk of irreparable harm to Plaintiff. (Reduced to \$700k on interlocutory appeal).

- **Dietz Development LLC v. Perez**, Fairfax County, VA Cir. Court No. CL 2012-16249, Oct. 2012.
 - Contractor filed suit seeking \$750k damages, injunctive relief for defamatory reviews on Yelp, Angie's List.
 - 12/5/12 - Court granted prelim. injunction in part and ordered defendant to delete/modify some statements.
 - Petition for Appellate Review filed to VA Supreme Court, still pending.

- **mLogica Inc. v. Karan**, Orange County, CA Sup. Court, April 30, 2012.
 - Suit for damages/injunctive relief for false blog/email claims that mLogica did not pay vendors, engaged in "unscrupulous, unethical and illegal conduct", and siphoned money from vendors/customers.
 - Defendant also sent claims to mLogica clients, using list obtained improperly from mLogica.
 - Company won a \$1.56m verdict and injunction. Case now pending on appeal.

- **Lynch v. Christie**, USDC Maine, Case # 2:11-cv-70, June 21, 2012.
 - Suit for damages/injunctive relief by chiropractor against a former patient and others, who claimed in on-line web page and on Facebook that Plaintiff sexually abused the patient.
 - Court issued \$100k pre-judgment attachment on defendant assets, based on likelihood Plaintiff will succeed on merits.
 - Pretrial memoranda filed March 8, 2013. On trial list for April 1, 2013.

Thank you!

Gregory G. Thiess
Vice President, Assistant General Counsel
Robert Bosch, LLC
Broadview, IL

Exhibit 1

Preventative Steps – Sample Social Media Policy

Available in Microsoft Word format at <http://usld.practicallaw.com/5-501-1524>.

Purpose

[EMPLOYER NAME] recognizes that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to [EMPLOYER NAME]'s confidential and proprietary information, reputation and brands, and can jeopardize the company's compliance with business rules and laws.

To minimize these business and legal risks, to avoid loss of productivity and distraction from employees' job performance and to ensure that the company's IT resources and communications systems are used only for appropriate business purposes, [EMPLOYER NAME] expects its employees to adhere to the following guidelines and rules regarding use of social media.

Compliance With Related Policies and Agreements

All of [EMPLOYER NAME]'s other policies that might apply to use of social media remain in full force and effect. Employees should always adhere to them when using social media. In particular, the following policies should be kept in mind: [LIST RELATED POLICIES AND AGREEMENTS IN BULLET FORM.]

Social media should never be used in a way that violates any other [EMPLOYER NAME] policies or employee obligations. For example, employees are prohibited from using social media to:

- Violate [EMPLOYER NAME]'s IT resources and communications systems policies.
- Violate [EMPLOYER NAME]'s confidentiality and proprietary rights policies.
- Circumvent [EMPLOYER NAME]'s ethics and standards of conduct policies.
- Defame or disparage [EMPLOYER NAME] or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders.
- Harass other employees in any way.
- Circumvent policies prohibiting unlawful discrimination against current employees or applicants for employment.
- Violate [EMPLOYER NAME]'s privacy policies (for example, never access private password protected sites of co-workers or other [EMPLOYER NAME] stakeholders without permission).

Exhibit 1

Preventative Steps – Sample Social Media Policy

Personal Use of Social Media

[Personal use of social media is never permitted on working time or by means of the company's computers, networks and other IT resources and communications systems.]

OR

[We recognize that employees might work long hours and occasionally may desire to use social media for personal activities at the office or by means of the company's computers, networks and other IT resources and communications systems. We authorize such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Neither is commercial, personal, religious or political solicitation, or promotion of outside organizations unrelated to company business.]

No Expectation of Privacy

All contents of the [EMPLOYER NAME]'s IT resources and communications systems are the property of the company. Therefore, employees should have no expectation of privacy whatsoever in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on the company's electronic information and communications systems.

You are expressly advised that in order to prevent misuse, **[EMPLOYER NAME] reserves the right to monitor, intercept and review, without further notice, every employee's activities using the company's IT resources and communications systems, including but not limited to social media postings and activities, and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the** monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The company also may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice. Do not use the company's IT resources and communications systems for any matter that you desire to be kept private or confidential from the company.

Exhibit 1

Preventative Steps – Sample Social Media Policy

Business Use of Social Media

If you are required to use social media as part of your job duties, for the company's marketing, public relations, recruitment, corporate communications or other business purposes, you should carefully review [EMPLOYER NAME]'s [NAME OF SOCIAL MEDIA BUSINESS USE GUIDELINES]. If your job duties require you to speak on behalf of the company in a social media environment, you must still seek approval for such communication from [YOUR MANAGER/DEPARTMENT NAME]. Likewise, if you are contacted for comment about [EMPLOYER NAME] for publication, including in any social media outlet, direct the inquiry to [DEPARTMENT NAME] and do not respond without written approval.

Guidelines for Employees' Responsible Use of Social Media

The above material covers specific rules, policies and contractual obligations that employees must follow in using social media, whether for personal or business purposes, in consideration of their employment and subject to discipline for violations. The following sections of the policy provide employees with common-sense guidelines and recommendations for using social media responsibly and safely, in the best interests of [EMPLOYER NAME]. These voluntary guidelines are intended to add to, not contradict, limit or replace, the applicable mandatory rules, policies and contractual obligations above.

Protect the Company's Goodwill, Brands and Business Reputation

The [EMPLOYER NAME]'s [EMPLOYEE HANDBOOK/CONFIDENTIALITY AND PROPRIETARY RIGHTS AGREEMENT] prohibits you from posting disparaging or defamatory statements about the company or its business interests (see above), but you should also avoid social media communications that might be misconstrued in a way that could damage the company's goodwill and business reputation, even indirectly.

You are personally responsible for what you communicate in social media. Remember that what you publish might be available to be read by the masses (including the company itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

If you disclose your affiliation as an employee of [EMPLOYER NAME], it is recommended that you also include a disclaimer that your views do not represent those of your employer. For example, consider such language as "the views in this posting do not represent the views of my employer".

Exhibit 1

Preventative Steps – Sample Social Media Policy

Respect Intellectual Property and Confidential Information

The [EMPLOYER NAME]'s [CONFIDENTIALITY AND PROPRIETARY RIGHTS AGREEMENT/EMPLOYEE HANDBOOK] restricts employees' use and disclosure of the company's confidential information and intellectual property (see above). Beyond these mandatory restrictions, you should treat the company's valuable trade secrets and other confidential information and intellectual property accordingly and not do anything to jeopardize them through your use of social media. In addition, you should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for yourself and for [EMPLOYER NAME].

Do not use the company's logos, brand names, taglines, slogans or other trademarks, or post any confidential or proprietary information of the company, without prior written permission from the [EMPLOYER NAME] legal department.

Respect Your Co-Workers and Other [EMPLOYER NAME] Stakeholders

Do not post anything that your co-workers or [EMPLOYER NAME]'s customers, clients, business partners, suppliers, vendors or other [EMPLOYER NAME]'s stakeholders would find offensive, including ethnic slurs, sexist comments, discriminatory comments, insults or obscenity.

Do not post anything related to your co-workers or [EMPLOYER NAME]'s customers, clients, business partners, suppliers, vendors or other [EMPLOYER NAME]'s stakeholders without their written permission.

ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

I have received and read a copy of the [EMPLOYER NAME] Social Media Policy and understand its contents. I understand that [EMPLOYER NAME] expressly reserves the right to change, modify or delete its provisions without notice.

_____ [EMPLOYEE NAME] _____ Date]

Footnotes

1. "Gartner sees huge rise in corporate social media monitoring". May 29, 2012, by Grant Gross, IDG News Service, http://www.computerworld.com/s/article/9227556/Gartner_sees_huge_rise_in_corporate_social_media_monitoring?taxonomyId=144&pageNumber=2.
2. "Jobvite 2012 Social Recruiting Survey Results", available at http://web.jobvite.com/rs/jobvite/images/Jobvite_2012_Social_Recruiting_Survey.pdf?mkt_tok=3RkMMJWWfF9wsRokvqvBZKXonjHpfX86uwrX6aylMI%2F0ER3fOvrPUfGjI4CSMdkl%2FqLazICFpZo2FFSFeKdDZRF. "Social Networking Statistics", at Statistics Brain, <http://www.statisticbrain.com/social-networking-statistics/>.
3. Id.
4. Id.
5. Id.
6. Id.
7. Press Release of Silkroad Technologies, covering its report titled "Social Media & Workplace Collaboration, 2012 Latest Practices, Key Findings, Hot Topics". Report published October 3, 2012, at <http://pages.silkroad.com/rs/silkroad/images/social-media-workplace-collaboration-silkroad-talenttalk-report.pdf>.
8. Id.
9. "Social Networking Statistics", at Statistics Brain, <http://www.statisticbrain.com/social-networking-statistics/>.
10. Id.
11. Id.
12. Report on LinkedIn web site, at <http://press.linkedin.com/about>.
13. "Social Networking Statistics", at Statistics Brain, <http://www.statisticbrain.com/social-networking-statistics/>.
14. Federal Trade Commission Press Release, at <http://www.ftc.gov/opa/2012/06/spokeo.shtm>.
15. Federal Trade Commission Guide, at <http://business.ftc.gov/documents/bus08-using-consumer-reports-what-employers-need-know>.
16. OFCCP News Release, at <http://www.dol.gov/opa/media/press/ofccp/OFCCP20120576.htm>.
17. OFCCP Directive No. 306, at <http://www.dol.gov/ofccp/regs/compliance/directives/dir306.htm>.
18. "Big Data: Businesses Wary of Analytics on Unknown Social Media Data Quality", by Dick Weisinger, Nov. 14, 2012, at <http://www.forrtek.com/blog/?p=3381>.
19. For a summary of state "Discrimination Laws Regarding Off-Duty Conduct", see the report of the National Conference of State Legislatures, at <http://www.ncsl.org/documents/employ/off-dutyconductdiscrimination.pdf>.
20. "Six states outlaw employer snooping on Facebook", by Dara Kerr, January 2, 2013, at http://news.cnet.com/8301-1023_3-57561743-93/six-states-outlaw-employer-snooping-on-facebook.
21. "Employee Abuse of Social Media in Compromising Employer Business Proprietary Information", by Kathleen Pohlid, DHPM, PC., at http://hotelexecutive.com/business__review/3321/employee-abuse-of-social-media-in-compromising-employer-business-proprietary-information.
22. "Report of the Acting General Counsel Concerning Social Media Cases", Office of the General Counsel, Division of Operations-Management, Aug. 18, 2011, at <http://www.nlr.gov/news/acting-general-counsel-releases-report-social-media-cases>.
23. "Report of the Acting General Counsel Concerning Social Media Cases", Office of the General Counsel, Division of Operations-Management, Jan. 24, 2012, at <http://www.nlr.gov/search/simple/document/om%20memo%20january%2024%2C%202012>.
24. "Report of the Acting General Counsel Concerning Social Media Cases", Office of the General Counsel, Division of Operations-Management, May 30, 2012, at <http://mynlrb.nlr.gov/link/document.aspx/09031d4580a375cd>.
25. "FTC's Updated .com Disclosures Guidance", by Jonathan L. Pompan and Ellen T. Berge, <http://www.jdsupra.com/legalnews/ftcs-updated-com-disclosures-guidance-53735/> (March 14, 2013).
26. FTC Press Release, March 12, 2013, at <http://www.business.ftc.gov/blog/2013/03/ftc-reboots-com-disclosures-four-key-points-and-one-possible-way-bypass-issue-altogethe>.
27. "Gartner Says By 2014, 10-15 Percent of Social Media Reviews to Be Fake, Paid for By Companies", Sept. 17, 2012, at <http://www.gartner.com/newsroom/id/2161315>.
28. Virtual World Law Blog, by Ian Schick, Pillsbury Winthrop Shaw Pittman LLP, Jan. 14, 2013, at <http://www.jdsupra.com/legalnews/endorsement-based-advertising-subject-to-81624/>. See also "Paying for Online Endorsements and the FTC View of Social Media Policy", by Lance Godard, January 17, 2013, at <http://socialmediatoday.com/lggodard/1164266/your-business-paying-online-endorsements-ftc-might-take-different-view>.