



MECKLER BULGER TILSON  
MARICK & PEARSON LLP

# An Investigator's Guide to Social Media

Jake Rubinstein

AIG Conference

May 19, 2011

# Social Media: Everyone Is Doing It

- Why investigators should pay attention to social media
  - 96% of people under age 30 have joined a social network
  - LinkedIn has 100 million users; Twitter has 75 million users
  - There are over 200 million individual blogs
  - Facebook has over 500 million active users who post over 60 million status updates per day

\*Source: *Socialnomics*, Eric Qualman, Wiley Pub. 2009

# What People Do On Social Media

- Criticize co-workers & supervisors
- Engage in harassment & bullying
  - Rutgers University student commits suicide after roommate posts video on Facebook of him having sex
  - Roommate was indicted on 15 counts including charges for hate crime, invasion of privacy and bias intimidation
  - Another student, facing lesser charges for invasion of privacy, was not named in the indictment, possibly indicating she is cooperating with the investigation
- Vent about their jobs
- Publish photos & videos
- State personal opinions on political and other issues

# Social Networking: Employee Discipline

- 15% of employers have disciplined an employee for violating multimedia sharing/posting policies.\*
- 17% of employers have disciplined an employee for violating blog or message board policies.\*
- 8% of employers have terminated an employee for Facebook or LinkedIn activity.\*
- 32% of employees do not use social networks for fear it will negatively affect their career.\*\*

\*Sources: Adam Ostrow, *FACEBOOK FIRED: 8% of US Companies Have Sacked Social Media Miscreants* (2009), <http://mashable.com/2009/08/10/social-media-misuse/> (a study of companies with 1,000 or more employees by Proofpoint, an Internet Security Firm).

\*\*Deloitte, *Trust in the Workplace: 2010 Ethics & Workplace Survey* (2010), [http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us\\_2010\\_Ethics\\_and\\_Workplace\\_Survey\\_report\\_071910.pdf](http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2010_Ethics_and_Workplace_Survey_report_071910.pdf).

# Some Examples Of Social Media-Related Internal Investigations

- February 11, 2010: South Carolina paramedic fired for creating & publishing on Facebook a 3-minute animated video spoof of cartoon doctor & paramedic responding to an emergency (source: [mediatakeout.com](http://mediatakeout.com))
- May 17, 2010: Waitress fired after posting a negative comment about two of her customers, calling them “cheap.” Although she didn’t name the customers, she named the restaurant where she worked. (source: [careerbuilder.com](http://careerbuilder.com))

# More Examples Of Social Media-Related Internal Investigations

- March 3, 2010: Professor at East Stroudsburg University in Pennsylvania fired after posting Facebook status updates such as “Does anyone know where I can find a very discrete hitman? Yes, it’s been that kind of day” (source: [mediatakeout.com](http://mediatakeout.com))
- June 10, 2010: Five California nurses terminated for violating patient privacy rules after they were found to have discussed patient cases on a social media site (source: [mediatakeout.com](http://mediatakeout.com))

# More Examples Of Social Media-Related Internal Investigations

- February 23, 2011: Indiana Deputy Attorney General fired for remarks made on Twitter suggesting that Wisconsin riot police should use live ammunition to clear protestors from the state capitol building. (source: usatoday.com)
- March 15, 2011: Comedian Gilbert Gottfried, voice of the AFLAC duck, was fired after making offensive jokes on Twitter regarding the recent events in Japan. (source: usatoday.com)

# Use of Social Media By Law Enforcement Agencies

- 81% of agencies report use of some form of social media
- 66.8% of agencies report having a Facebook page
- 62.3% of agencies report using social media for criminal investigations
- 40.0% of agencies report using social media to solicit tips
- Other reported uses by law enforcement:
  - Digital “wanted” posters
  - Twitter chats or postings used to monitor gang/group conduct
  - Fake profiles used to infiltrate gangs
  - Posted photos used as evidence

\*Source: International Association of Chiefs of Police, Social Media Survey (2010), [www.iacpsocialmedia.org](http://www.iacpsocialmedia.org)

# How Might You Use Social Media As An Investigative Tool?

- Investigating Complaints
- Learning About Complainants
- Learning About Witnesses
- Learning About the Accused

# Legal Risks of Using Social Media as an Investigative Tool

- Fact Pattern: A Highway Department employee creates a password protected social media site as a forum for fellow employees to “vent” about working for the Highway Department
- You receive a complaint about statements made on this social media site, including employees bragging about performing political work on Highway Department time

# Legal Risks of Using Social Media as an Investigative Tool

- You obtain the username and password from a cooperating witness who is an invited member of this site and discover incriminating evidence pointing to political discrimination, timecard fraud and official misconduct
- Before taking action, consider how the site was set up (*i.e.*, invitation to join only) and how you obtained access.
- Accessing this site during your investigation could result in claims under state privacy laws, the Electronic Communications Privacy Act, and/or the Stored Communications Act. *Pietrylo v. Hillstone Rest. Group* (employer accessing site violated the federal Stored Communications Act and New Jersey law).

# How Do I Get Access To A Social Media User's Site?

- If Privacy Settings Allow Public Access
  - Simply visit the site
  - Yes, it's that easy!
- If Privacy Settings Block Public Access
  - You will need a subpoena
  - For Facebook, it must be a valid California subpoena



# DISCUSSION AND QUESTIONS