FENWICK & WEST LLP

SILICON VALLEY CENTER 801 CALIFORNIA STREET MOUNTAIN VIEW, CA 94041

TEL 650.988.8500 FAX 650.938.5200 WWW.FENWICK.COM

NATIONAL EMPLOYMENT LAW INSTITUTE

35th Annual PUBLIC SECTOR EEO & EMPLOYMENT LAW CONFERENCE

August 2015 – San Francisco, CA

eWorkplace Policies Restricting Employees' Acceptable Use of Technology, Social Media & The Cloud

Robert D. Brownstone, Esq.*

**Robert D. Brownstone* is the Technology & eDiscovery Counsel and Chair of the Electronic-Information-Management (EIM) Practice Group at *Fenwick & West LLP*, where he has spent more than half of his 28 year lawyer career. He advises clients on: information-security; privacy; "eWorkplace" policies; social media risks and rewards; eDiscovery; and retention/destruction policies and protocols.

A prolific nationwide advisor, speaker and writer for many years, Bob is frequently quoted in the press on electronic information issues. Check out his blog at <www.ITLawToday.com>. He also has taught Electronic Discovery Law & Process classes at four different law schools since 2009 and has been on the NELI Advisory Board since 2008. ***The August 20 presentation will be his 72nd for NELI since 2002.***

For Bob's full biography and extensive bibliography, *see* <fenwick.com/bobbrownstone> and <fenwick.com/bobbrownstoneinsights>.

THESE MATERIALS ARE MEANT TO ASSIST IN A GENERAL UNDERSTANDING OF THE CURRENT LAW RELATING TO PRIVACY AND ELECTRONIC INFORMATION MANAGEMENT. THEY ARE NOT TO BE REGARDED AS LEGAL ADVICE. ORGANIZATIONS OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

eWorkplace Policies Restricting Employees' Acceptable Use of Technology, Social Media & The Cloud

Materials – TABLE OF CONTENTS

PAGE

PAPER

APPENDICES

Table of Contents

TABLE OF CONTENTS *(c't'd)*

Page(s)

TABLE OF CONTENTS *(c't'd)*

TABLE OF CONTENTS *(c't'd)*

IMPORTANT NOTE:

The most current iteration of this White Paper is posted periodically at <http://tinyurl.com/eWorkplaceMaterialsLatestFWLPP>. This version ("**Brownstone eWorkplace IV**") is the fourth in a series by the author over the past eight years. For most every topic covered herein, you can find a corresponding discussion of older authorities in each of the previous three "episodes", listed here in reverse chronological order:

- *The eWorkplace – Access, Security and Privacy in the Era of "The Cloud," Social Media and BYOD* **(Feb. 13, 2014)** <itlawtoday.com/files/2014/05/eWorkplace_Materials_2-12-14_©_Brownstone_FWLPP.pdf> ("**Brownstone eWorkplace III**")
- *eWorkplace Policies – Social-Media, Privacy & Internet-Security* **(Apr. 3, 2012)** <fenwick.Com/fenwickdocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf> ("**Brownstone eWorkplace II**")
- *Workplace Privacy Policies* **(Aug. 11, 2009)** <fenwick.com/fenwickdocuments/eworkplace_policies_materials_public_sector_eeo_8-28-09.pdf> (**"Brownstone eWorkplace I"** or **"Brownstone eWorkplace"**)

I. OVERVIEW – THE MODERN LANDSCAPE

A. Physical Conduct PLUS Digital Activity

Traditional concerns for employers have included: conduct leading to liability to third-parties; "frolic and detour" or other slacking; and protection of trade secrets. Over the past fifteen years, workplaces have become increasingly digitized, as a ramification of electronic information's predominance in all aspects of modern life.

We live in an era when the universe of communication platforms is ever-expanding. The omnipresence of Web 2.0 and User-Generated Content (UGC) – blogs, wikis, social networking sites and microblogging sites such as Twitter – has forged a brave new world. In this context, a single negligent or malicious employee can cause truly irreparable harm.

Three kinds of conduct should be of concern to employers. Many a problematic incident involves completely unintentional conduct[1] on the part of an executive or a staff member. At the other end of the spectrum lie those actions that the author likes to call "intentionally harmful intentional disclosures." The trickiest category arguably sits in the middle, entailing what the author has dubbed "*inadvertently* harmful *intentional*

[1] Examples include losing laptops, using poor passwords and "clicking on a malicious link found in a phishing message." Marcos Colón, *"Human error" contributes to nearly all cyber incidents, study finds*, SC Magazine (June 16, 2004) <scmagazine.com/human-error-contributes-to-nearly-all-cyber-incidents-study-finds/printarticle/356015/> (discussing *IBM Security Services 2014 Cyber Security Intelligence Index*, (June 9, 2014) ("*[a]nalysis of cyber attack and incident data from IBM's worldwide security operations*") <media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf>.

disclosures." So-called "Netiquette" violations continue to burgeon and thus comprise the focus of much of this White Paper.

Against that backdrop, though, employers now have many more legitimate reasons to monitor their employees' electronic communications in the workplace. Web surfing to loll away the day[2] can be tracked. In addition, Seemingly with each passing day, new methods emerge – including within the "Internet of Things" ("IoT")[3] – that can monitor individuals at work, in their homes and even in their cars.[4]

---

[2] Alana Semuels, *Man reportedly outsources his own job to China, watches cat videos*, L.A. Times (Jan. 17, 2013) <http://articles.latimes.com/print/2013/jan/17/business/la-fi-mo-man-outsourced-job-to-china-20130117>.

[3] *See* these two search engines: <https://thingful.net/>; and <https://www.shodan.io/>. *See also* Robert D. Brownstone, et al., *Wearables, IoT and Social Media . . . Oh My!,* at 3, 6-7 and 17-18, ALM LTWC (July 14, 2015) (linking to many IoT resources) <http://www.itlawtoday.com/files/2015/07/IoT-ARMA-IG-LTWC-7-14-15-c-FWLPP-et-al.pdf>; Robert D. Brownstone, *A "Wearables" Carol – Beware The Three Ghosts*, Digital Mountain E-Newsletter (May 27, 2015) <http://digitalmountain.com/enews/SPRING_2015_Article3.pdf> (citing many other IOT articles); Brian Wasson, *Internet of Things* <http://www.wassom.com/tag/internet-of-things> (last visited March 1, 2015); Mike Haberman, *The "Internet of Things" and the Clash With Employee Privacy*, Blogging4Jobs (May 19, 2014) <www.blogging4jobs.com/hr/internet-things-clash-employee-privacy>; Joe Mont, *Regulating the 'Internet of Things*,' Compliance Week (May 6, 2014) <http://www.complianceweek.com/news/alert/regulating-the-internet-of-things>; Allison Grande, *Smart Fridges Head From Kitchen To Courtroom*, law360 (Apr. 4, 2014) <www.law360.com/articles/524831/smart-fridges-head-from-kitchen-to-courtroom> (subscription needed); Sean Martin, *Who Will Pay the Price When Tragedy Strikes the IoT?* Law Technology News (LTN) ("The Internet of Things facilitates communication, whether or not illicit") (March 20, 2014) <www.lawtechnologynews.com/id=1202647721399/Who-Will-Pay-the-Price-When-Tragedy-Strikes-the-IoT%3Fmcode=0&curindex=0&curpage=ALL> (subscription needed); Rachel Teisch, *How the 'Internet of Things' Will Impact Data Security and Privacy*, JD Supra Business Advisor (Mar. 6, 2014) <www.jdsupra.com/legalnews/how-the-internet-of-things-will-impact-07266/>; Federal Trade Commission (FTC), *Internet of Things - Privacy and Security in a Connected World*, FTC (Nov. 19, 2013) <www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

[4] *See Cunningham v. N.Y.S. DOL*, 21 N.Y. 3d 515, 997 N.E. 2d 468 (2013) <http://www.nycourts.gov/ctapps/Decisions/2013/Jun13/123opn13-Decision.pdf>, discussed in **Section II(B(1)(d)(i)** below. *See also* Derek S. Whitefield, Dmitriy Kopelevich and Isabella C. Hsu, *Automobile Data Recording Is Not An Invasion Of Privacy*, law360 (June 19, 2014) <http://tinyurl.com/Auto-Data-Recording-Dykema>; Ali Winston, *Plans to expand scope of license-plate readers alarm privacy advocates*, The Center for Investigative Reporting ("CIR") (June 17, 2014) <cironline.org/reports/plans-expand-scope-license-plate-readers-alarm-privacy-advocates-6451>; Nancy Libin, *Connected Cars Collide With Consumer Privacy*, law360 (Apr. 17, 2014) <www.law360.com/articles/527707/connected-cars-collide-with-consumer-privacy> (subscription needed) Jaclyn Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. Times (Jan. 10, 2014) <nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html>; Spencer E. Ante and Lauren Weber, *Memo to Workers: The Boss Is Watching; Tracking Technology Shakes Up the Workplace*, WSJ (Oct. 22, 2013) (telematics) <online.wsj.com/news/articles/SB10001424052702303672404579151440488919138> (subscription needed); *Event data recorders installed in cars stirring controversy*, KTVU News (July 12, 2012) <http://web.archive.org/web/20121103061105/http://www.ktvu.com/news/news/crime-law/event-data-recorders-installed-cars-stirring-contr/nPrZD/>; Christopher Maag, *Tracking Thieves, or Teens; Technology, the Stealthy Tattletale*, N.Y. Times (Oct. 27, 2007) <www.nytimes.com/2007/10/27/technology/27tracking.html?_r=1&pagewanted=print>.

While employers, in pursuing legitimate objectives, may make various intrusions into their employees' privacy, there are nevertheless some limitations on what employers may do. Thus, some potential legal pitfalls await employers that go too far. It is not easy to tame the three-headed compliance monster discussed in Section V(A)(1) below.

B. Strange Things People Memorialize – Overview of Liability Risks

In this century, e-mail messages – and other types of digital gaffes – continue to become more pivotal in litigation and in the court of public opinion. Examples of well-known figures laid low in the last year include New Jersey Governor Chris Christie (and staff)[5] and former Federal Circuit Court of Appeals Chief Judge Randall Rader.[6]

1. Employees' Damaging Emails

In today's world, one regularly learns of pivotal "smoking guns" e-mails or other kinds of damaging electronic-communications in business, national politics and local politics. Examples of "loose lips" coming home to roost long after the fact include:

- "Deflategate texts" by Tom Brady and other New England Patriots employees <online.wsj.com/public/resources/documents/Deflategate.pdf>;
- Sony executives' emails disparaging President Obama, Angelina Jolie and a myriad of others <https://wikileaks.org/sony/emails/>;
- leaders of the now defunct Dewey & LeBoeuf law firm who have been

---

[5] Heather Haddon, *Special Grand Jury Impaneled in Bridge Probe*, WSJ. (June 6, 2014) <http://www.wsj.com/articles/special-grand-jury-impaneled-in-bridge-probe-1402283558>; *Christie Faces Political Fallout Over GWB Lane Closure Aides Ordered*, Voz Is Neias? (Jan 9, 2014) (including image of infamous email) <vosizneias.com/151753/2014/01/09/fort-lee-nj-christie-faces-political-fallout-over-gwb-lane-closure/>.

[6] *In re Reines*, 771 F.3d 1326 (Fed. Cir. Nov.5, 2014) (per curiam reprimand of litigator for sharing judge's laudatory email) <http://www.cafc.uscourts.gov/images/stories/opinions-orders/14-ma004.pdf>; Ashby Jones, *Email Controversy Leads to Reprimand of Weil Gotshal Patent Lawyer*, WSJ Law Blog (Nov. 5, 2014) <http://blogs.wsj.com/law/2014/11/05/email-controversy-leads-to-reprimand-of-weil-gotshal-patent-lawyer/>; Scott Graham, *Federal Circuit Reprimands Reines for Sharing Rader Compliments With Clients*, The Recorder (Nov. 5, 2014) <http://www.therecorder.com/id=1202675620589/Federal-Circuit-Reprimands-Reines-for-Sharing-Rader-Compliments-With-Clients> (subscription needed); Scott Graham, *Rader Leaves Federal Circuit With Unfinished Business*, Recorder (June 30, 2014) ("Rader resigned as chief judge last month and ultimately from the court altogether while issuing an open apology to his colleagues for an effusive email to Weil, Gotshal & Manges partner Edward Reines that could have been read as an open endorsement of Reines' skills") <therecorder.com/id=1202661498409/Rader-Leaves-Federal-Circuit-With-Unfinished-Business%3Fmcode=0&curindex=0&curpage=ALL> (subscription needed); Joe Mullin, *Top US patent judge resigns following "ethical breach,"* Ars Technica (June 16, 2014) ("[a]n e-mail highlighting praise for an attorney's argument led to resignation") <arstechnica.com/tech-policy/2014/06/top-us-patent-judge-resigns-following-ethical-breach>; Scott Graham, *Rader Steps Down as Chief, Apologizes for Reines Email*, The Recorder (May 23, 2014) <therecorder.com/id=1202656698314/Rader%20Steps%20Down%20as%20Chief%20Apologizes%20for%20Reines%20Email?mcode=0&curindex=0&curpage=ALL> (subscription needed) (linking to his May 23, 2014 open letter of apology to his colleagues <cafc.uscourts.gov/images/stories/5-23-14_RRR%20_Letter.pdf>).

indicted for accounting fraud based in part on emails containing phrases such as "*cooking the books*, *fake income*, and *clueless auditor*;"[7] and

- Intel Corp., which is still defending a 10-year old lawsuit ostensibly in part because of very old "internal Intel presentation slides and emails, some of which instruct the recipients to 'do not forward' and 'delete after today's meeting.'"[8]

Knowledge of, and indifference to, inappropriate conduct are often memorialized as well. In harassment or discrimination cases, one or two explicit messages can bolster other evidence of hostile environment or discrimination. In the hostile environment context, some courts have found that, even if a pertinent social-media page belongs to a co-worker of Plaintiff, the employer can still be responsible for remedying harassing behavior in any setting that is related to the workplace.[9]

2. Employees' Damaging Internet Use and Postings

In addition to e-mail, Internet content and postings – on blogs, wikis, social networking sites, Twitter, etc. – present risk-management challenges. Both incoming and outbound data present challenges to employers.

a. Internet Activity

Employee web-surfing can entail visiting pornographic websites and/or sending inapt emails,[10] not only cutting into productivity but also potentially creating a hostile

---

[7] Daniela Guzman, *Dewey execs indicted for fraud learn first rule of e-discovery – it's the email, stupid*, ACEDS (Mar. 13, 2014) <http://www.aceds.org/dewey-execs-indicted-on-fraud-learn-first-rule-of-e-discovery-its-the-email-stupid/>.

[8] Marisa Kendall, "'*Blunt' Emails Dog Intel in Pentium 4 Class Action*," Recorder (Apr. 11, 2014) <therecorder.com/id=1202650895865/Blunt+Emails+Dog+Intel+in+Pentium+4+Class+Action%3Fmcode=0&curindex=0&curpage=ALL> (subscription needed).

[9] *See, e.g., Amira–Jabbar v. Travel Servs., Inc.*, 726 F. Supp. 2d 77. 87, 93 (D. P.R. Sep. 10, 2010) (once Facebook posting brought to attention of employer, blocking Facebook access for all office computers was adequate remedial response) <https://cases.justia.com/federal/district-courts/puerto-rico/prdce/3:2008cv02408/71930/61/0.pdf>.

See also Espinoza v. County of Orange, 2012 WL 420149 (Cal. App. 4 Dist.), 26 A.D. Cases 31 (Cal. App. 4 Dist. Mar. 12, 2012) (unpublished, non-citable decision as to anonymous derogatory posts that employer had concluded were from co-workers and were made on a co-worker's blog accessed from workplace computers) <http://tinyurl.com/Espinosa-Orange-3-12-12> (citing pre-social media case of *Blakey v. Continental Airlines*, *Inc.*, 164 N.J. 38, 751 A.2d 538 (2000) <http://caselaw.findlaw.com/nj-supreme-court/1044008.html>); David L. Martin and Christopher C. Hosselman, *Social Media Creates New Sources of Liability for Employers*, L.A.D.J. (Sep. 18, 2012) <wshblaw.com/wp-content/uploads/2012/10/SocialMediaCreatesNewSourcesforLiabilityforEmployeers.pdf>.

[10] *Sheriff's deputy accidentally e-mails female deputies' bra cup sizes to all members of the department*, Office of Inadequate Security (Oct. 25, 2013) <www.databreaches.net/ga-sheriffs-deputy-accidentally-e-mails-female-deputies-bra-cup-sizes-to-all-members-of-the-department/>

work environment and/or criminal liability for knowing possession of contraband. Moreover, innocent yet ill-advised web activity and/or naiveté as to "social engineering" can also cause serious security breaches for employers.[11] Lurking potential dangers include [spear-]phishing and/or whaling schemes and other types of social engineering[12] as well as e-mail messages containing malware and/or links to malicious websites.[13] Employees' use of social networking sites increases employees *and* employers' vulnerability to malware.

Unintentional conduct can readily put employees' and/or customers'/ patients' personally identifiable information[14] or health/medical/insurance information[15] at risk – thus

---

[11] Ralph Losey, *U.S. Employees Are Weakest Link In America's Cybersecurity - **Part One***, e-Discovery Team (May 27, 2014) <http://e-discoveryteam.com/2014/05/27/u-s-employees-are-weakest-link-in-americas-cybersecurity-part-one/>.

[12] Taylor Armerding, The human OS: Overdue for a social engineering patch, CSO (Oct, 13, 2104) <www.csoonline.com/article/2824563/social-engineering/the-human-os-overdue-for-a-social-engineering-patch.html>; Aliya Sternstein, Nextgov, *Fake Dot-Gov Webmail Used in Phishing Scam to Hack EPA and Census Staff* (June 12, 2014) <nextgov.com/cybersecurity/2014/06/fake-dot-gov-webmail-used-phishing-scam-hack-epa-and-census-staff/86374/>; Malcovery Security, *Top 10 Phished Brands*, Re-Soft (Apr. 17, 2014) ("Most Phished Brands 'Missed' by AntiVirus Based on Big Data Security Intelligence Q1 2014") <resoftco.com/datasheets/Top_Phished_BrandsQ1_2014_Malcovery_Security_Final.pdf>; Ralph Losey, *U.S. Employees Are Weakest Link In America's Cybersecurity - **Part Two**,* e-Discovery Team (June 2, 2014) <e-discoveryteam.com/2014/06/02/u-s-employees-are-weakest-link-in-americas-cybersecurity-part-two/>.

[13] *See generally* the various short but powerful FBI "Counterintelligence Brochures" posted at <http://www.fbi.gov/about-us/investigate/counterintelligence/counterintelligence-brochure>. *See also* the resources linked from **Slide 32 of Appendix B**.

[14] 47 states plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands have notice of breach statutes as to PII. For a great compilation of cites/links to all of those sets of laws, including the most recent ones from Kentucky) *see* Nat'l Conf. of State Legislatures ("NCSL"), SECURITY BREACH NOTIFICATION (last updated Jan. 12, 2015) <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

[15] The reach of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) was expanded in February 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was, in turn, enacted as part of the American Recovery and Reinvestment Act of 2009. U.S. Dep't of Health and Human Services ("HHS"), *Health Information Privacy* <hhs.gov/ocr/privacy/index.html> (last visited June 29, 2014). September 23, 2013 marked the effective date of HHS' final regulations under HITECH. Omnibus HIPAA Rulemaking, Final Rule (Sep. 23, 2013) <hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html>.

For an excellent overview of the ramifications for employers, *see* Philip Gordon, *What Do Employers Really Need to Know About the New HIPAA/HITECH Omnibus Final Rule?* Littler (Feb. 5, 2013) <littler.com/publication-press/publication/what-do-employers-really-need-know-about-new-hipaahitech-omnibus-final>.

In addition to the HIPAA expansion, there are now at least seven states that have enacted data-breach statutes and/or regulations relating to medical, health and/or health-insurance information: Arizona, California, Connecticut (though only applying to insurers) Missouri, Nevada, North Dakota and Texas. *See* Baker Hostetler, *DATA BREACH CHARTS* (June 25, 2014) <bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf>.

leading to legal liability. Data breaches regularly occur in droves.[16] In May 2014, the U.S. Dep't of Health and Human Services (HHS) levied its biggest fine ever -- $4.8 million -- in a settlement with "New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of [electronic protected health information, a/k/a] ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results."[17]

In addition, publicized examples of *intentional* inapt exposure of medical/health information have been coming to the fore fairly regularly.[18] In one bizarre New York case, a medical facility was able to escape vicarious liability for breach of the common law "fiduciary duty of confidentiality" by a non-physician where:

> A nurse employed by [Defendant] Clinic recognized [Plaintiff] Doe as the boyfriend of her sister-in-law. The nurse accessed Doe's medical records and learned that he was being treated for the STD. While Doe was still awaiting treatment, she sent text messages to her sister-in-law informing her of Doe's condition. The sister-in-law immediately forwarded the

---

[16] *See* Privacy Rights Clearing House, *Chronology of Data Breaches Security Breaches 2005 – Present* (Apr. 20, 2015) (≈ 828 million records in ≈ 4,500 incidents since April 20, 2005) <www.privacyrights.org/data-breach>. *See also* Robert Westervelt, *Coca-Cola Laptop Breach A Common Failure Of Encryption, Security Basics*, CRN (Jan. 27, 2014) <www.crn.com/news/security/240165711/coca-cola-laptop-breach-a-common-failure-of-encryption-security-basics.htm>; Elizabeth A. Harris, Nicole Perlroth and Nathaniel Popper, *Neiman Marcus Data Breach Worse Than First Said*, N.Y. Times (Jan. 23, 2014) <nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html>; Elizabeth A. Harris and Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. Times (Jan. 10, 2014) <nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html>.

[17] HHS Press Office, *Data breach results in $4.8 million HIPAA settlements*, HHS Release (May 7, 2014) (linking to both Resolution Agreements) <www.hhs.gov/news/press/2014pres/05/20140507b.html>. *See also* Jaclyn Jaeger, *HHS Coming Down Harder on Healthcare Privacy Violations*, Compliance Week (June 10, 2014) <http://www.complianceweek.com/hhs-coming-down-harder-on-healthcare-privacy-violations/article/351305>.

[18] Natasha Singer, *Revelations by AOL Boss Raise Fears Over Privacy*, N.Y. Times (Feb. 10, 2014) <http://www.nytimes.com/2014/02/11/business/media/revelations-by-aol-boss-raise-fears-over-privacy.html>; Venkat Balasubramani, *Nurse Properly Fired and Denied Unemployment Due to Facebook Rant*, Technology & Marketing Law Blog (Jan. 13, 2014) <http://tinyurl.com/Goldman-Blog-Seton> (discussing *Guevarra v. Seton Med. Ctr.*, No. C. 13-2267 CW, 2013 WL 6235352 (N.D. Cal. Dec. 2, 2013) <cases.justia.com/federal/district-courts/california/candce/4:2013cv02267/266304/41/0.pdf>; *Fury as self-styled FDNY 'Bad Lieutenant' is and colleagues caught uploading graphic pictures of victims in 'web gore' galleries*, Daily Mail (Mar. 31, 2013) <www.dailymail.co.uk/news/article-2301961/Timothy-Dluhos-EMTs-uploading-graphic-pictures-suffering-victims-web-gore-galleries.html>; *Palleschi v. Cassano*, 102 A.D. 3d 603, 959 N.Y.S.2d 56 (A.D. 1 Dept. 2013) (upholding termination of Fire Dep't EMS Supervisor/Lieutenant who had uploaded "computer screen . . . concerning a 911 . . . gynecological emergency") <www.nycourts.gov/reporter/3dseries/2013/2013_00437.htm>; Virginia Henschel, *Facebook Terminations: Friends Don't Let Friends Talk Smack About Their Job*, LexisNexis Applied Discovery (Apr. 12, 2010) <http://tinyurl.com/Henschel-FB>.

> messages to Doe; according to Doe, the messages suggested that staff members were making fun of his medical condition.[19]

However, there New York's highest court did find that:

> where an injured plaintiff's cause of action fails because the employee is acting outside the scope of employment, a direct cause of action against the medical corporation for its own conduct, be it negligent hiring, supervision or other negligence, may still be maintained. . . . A medical corporation may also be liable in tort for failing to establish adequate policies and procedures to safeguard the confidentiality of patient information or to train their employees to properly discharge their duties under those policies and procedures.[20]

The ever-growing Cloud presents many thorny problems, as individuals and organizations' departments often store files and data at sites such as Dropbox, Hightail (formerly YouSendIt), Box and the like.[21] Yet, even centralized, administratively-controlled use of Google Apps for Business can present risk-management and/regulatory issues. For example, a university hospital (also a medical-school) decided that Google's boilerplate agreement did not comport with HIPAA's / HITECH's Business Associate Agreement (BAA) requirements. Thus, given that patients; protected health information (PHI) was being transmitted and maintained in Gmail and Google Drive, the hospital decided to give notice of breach to those affected -- even though there was no indication that the underlying sensitive information had been compromised.[22]

---

[19] *Doe v. Guthrie Clinic, Ltd*., 740 F.3d 864, 865 (2d Cir. 2014) (affirming dismissal of patient's claim for breach of the fiduciary duty of confidentiality based on New York State's highest court's answer to certified question) <ca2.uscourts.gov/decisions/isysquery/f0fe1e9f-9612-46b0-ab24-6459c62b09d9/1/doc/12-1045o_opn.pdf>; *Doe v. Guthrie Clinic, Ltd*., 22 N.Y. 3d 48, 982 N.Y.S. 2d 4, 15 N.E. 3d 578, 579-80 (2014) (finding "a medical corporation's duty of safekeeping a patient's confidential medical information is limited to those risks that are reasonably foreseeable and to actions within the scope of employment") <nycourts.gov/ctapps/Decisions/2014/Jan14/224opn14-Decision.pdf>.

[20] *Doe v. Guthrie*, 15 N.E. 3d at 581.

[21] Sharon Gaudin, *Business users bypass IT and go rogue to the cloud*, ComputerWorld (May 27, 2014) <http://www.computerworld.com/article/2489832/cloud-computing/business-users-bypass-it-and-go-rogue-to-the-cloud.html>.

[22] Oregon Health & Science University ("OHSU"), *OHSU notifies patients of 'cloud' health information storage*, OHSU News (July 28, 2013) <www.ohsu.edu/xd/about/news_events/news/2013/07-28-ohsu-notifies-patients-o.cfm>; Patrick Ouellette, *OHSU alerts patients of Google cloud security concerns*, Health IT Security (July 29, 2013) <http://healthitsecurity.com/2013/07/29/ohsu-alerts-patients-of-google-cloud-security-concerns/>.

b. Posts on Blogs, Wikis, Social Networking Sites, etc.[23]

i. Day-to-day Issues

A. General

The various 21st century platforms mentioned in Section I above raise many potential legal liability issues. As we all know, millions of workers now make extraordinarily prolific use of smartphones and social-networking. Organizations of all shapes and sizes are reaping the many rewards of social-networking sites (SNS) sites and applications. Even many organizations that are very risk-averse have realized that deciding whether to allow employees to use social-media at work is not just an all-or-nothing question. A growing tool set enables a more granular approach to balancing rewards and risks.

As to risk, the ramifications for employers from the content of employee blogs or sites or from leaks to non-employee blogs or sites include: intentional or unintentional disclosure of confidential information; and vicarious liability for content claimed to be harassing or otherwise actionable.

Anyone can now *instantly* become a publisher; and also there is a very good chance that any publicly available social-media page will be readily findable by standard web search engines.[24] Moreover, Twitter's own search engine <https://twitter.com/search-advanced> is readily available without logging into Twitter – or even having a Twitter account.[25] Even when blog pages, wiki pages or the like have been removed by the original author, their content may live on in, *e.g.*, The Wayback Machine, a/k/a The Internet Archive <https://archive.org/web/>. Plus, the elephant in the room is that many folks may have captured content as soon as it was posted.

Individuals' lack of facility with the ever-changing privacy settings[26] combines with the abilities of others to post about those individuals to open all social-media users to a lack of content control. Examples include:

---

[23] Those interested in the growing body of **social-media ethical prohibitions** as to lawyers, jurors and judges should use the Bibliography linked as **Item # 5 of Appendix A**. That bibliography is also available and maintained at <http://tinyurl.com/SocialMediaEthicsLatestFWLPP>.

[24] Stosh Jonjak, *Searching Social Media | Part 1: Googling Facebook*, iBrary Guy (May 8, 2014) <http://ibraryguy2.wordpress.com/2014/05/08/searching-social-media-pt1/>.

[25] Stosh Jonjak, *Searching Social Media | Part 2: Twitter*, iBrary Guy (May 22, 2014) <http://ibraryguy2.wordpress.com/2014/05/22/searching-social-media-part-2-twitter/>.

[26] *See, e.g.,* Violet Blue, *Facebook turns user tracking 'bug' into data mining 'feature' for advertisers*, ZDNet (June 17, 2014) <zdnet.com/facebook-turns-user-tracking-bug-into-data-mining-feature-for-advertisers-7000030603/>; Vindu Goel, *Some Privacy, Please? Facebook, Under Pressure, Gets the Message*, N.Y. Times (May 22, 2014) <www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html>; Minh Uong, *Flipping the Switches on Facebook's Privacy Controls*, N.Y. Times (Jan. 29, 2014) <www.nytimes.com/2014/01/30/technology/personaltech/on-facebook-deciding-who-knows-youre-a-dog.html>.

- posting photos and videos – including via the Vine app[27] – and/or tagging them – or others' photos and videos – with the names of co-workers and customers;

- LinkedIn features that not only readily enable end-runs around HR prohibitions on providing references/recommendations but also, by default, leave a trail each time a LinkedIn user has visited another user's profile; and [28]

- aspects of various social-media websites and apps that supposedly pull names and email addresses from users' Contacts lists.[29]

Thus, in turn, employers' risks of damaging disclosures have thus greatly increased at the same time as their ability to control content has decreased.

In any event, once someone has disseminated a message or image, all kinds of ramifications can ensue. For example, a teenager's bragging about her father's monetary settlement in an employment dispute led to a breach of the settlement agreement's confidentiality provision – and thus to a forfeiture of $80,000 of the $150,000 agreed upon

---

[27] Jacob Gershman, *The Latest Social Media Concern for Employer*s, WSJ Law Blog (May 21, 2013) <http://blogs.wsj.com/law/2013/05/21/the-latest-social-media-concern-for-employers/>.

[28] L.M. Sixel, *Online references come with pitfalls*, Houston Chronicle (Jan. 8, 2014) (citing an interviewee for the view that "[a]nother pitfall is that LinkedIn recommendations can be so specific that they inadvertently give away trade secrets[;] . . . [f]or example . . . a company may try to argue that a former employee took advantage of confidential information in trying to win business with former customers") <http://www.houstonchronicle.com/business/columnists/sixel/article/Online-references-come-with-pitfalls-5126014.php>; LinkedIn, *"Who's Viewed Your Profile" - Overview and Privacy* (January 7, 2015) <http://help.linkedin.com/app/answers/detail/a_id/42>; LinkedIn Settings, "Select what others see when you've viewed their profile" at <http://www.linkedin.com/settings> (last visited July 1, 2014) (LinkedIn login/password needed); Heather M. Sager, *Why Can't We Be 'Friends'?* The Recorder (July 27, 2012), available at .pdf p. 5 at <http://pdfserver.amlaw.com/ca/Special%20Report-Privacy_2012.pdf>; Tresa Baldas, *Lawyers warn employers against giving glowing reviews on LinkedIn*, Nat'l L.J. (July 6, 2009) <http://www.nationallawjournal.com/id=1202432039774/Lawyers-warn-employers-against-giving-glowing-reviews-on-LinkedIn>(subscription needed).

[29] *See, e.g., Perkins v. LinkedIn Corp.*, No. 13-cv-04303-LHK, 2014 WL 2751053 (N.D. Cal. June 12, 2014) (granting in part and denying in part – with leave to amend – motion to dismiss class action claims based on allegations of "harvesting and collecting email addresses from the users' contact lists" and inapt sending of endorsement requests) <cases.justia.com/federal/district-courts/california/candce/5:2013cv04303/270092/47/0.pdf>; *USA v. Path., Inc.*, Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief, 3:13-cv-00448-RS (N.D. Cal. Feb. 2, 2013) <http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc> (settlement based on allegations in FTC's Complaint, including contention that "Defendant violated the FTC Act by making deceptive representations through its application's user interface regarding the automatic collection of information from consumers' mobile device address books").

payout.[30] By way of additional example, in 2012, there was Florida state senator Peter Nehr who had sent shirtless photos of himself, only to find them posted on a political blog site.[31] Nehr's explanation was that he was just demonstrating to friends his extraordinary weight loss as he battled diabetes. But a few months later, the voters judged Nehr harshly, replacing the incumbent with a candidate who had lost two prior head-to-head battles with Nehr.[32]

As to recent employer trends, a major law firm's 2014 survey[33] concluded that there has been a big increase in each of the following:

- "businesses now us[ing] social media for business purposes;"
- "[s]ocial media misuse in the workplace";
- "disciplinary action against employees for misuse"; and
- "the number of businesses taking measures to stop employees from using social media at work."

Each employer, whether in the private or public sector needs to decide how aggressive or lenient to be as to employees' social-media use.

B. Private Sector

(i) Liability Risks

Employees' social-media posts may result in an employer's vicarious liability or in direct organizational liability -- especially in certain industries -- under: Federal antitrust laws; Federal securities laws; FTC online-advertising guidelines as to endorsements and testimonials (requiring that any testimonials or endorsements as to a company's product by an employee or by an insider – friends, family, beta tester, etc. – of such employee must identify the person's company connection); and/or industry-specific rules, such as:

---

[30] *Gulliver Schools v. Snay*, No. 3D13-1952, 2014 WL 769030 (Fla. 3 DCA Feb, 26, 2014) ("before the ink was dry on the agreement, and notwithstanding the clear language . . . mandating confidentiality, [Plaintiff – the former headmaster at Defendant/school --] violated the agreement by doing exactly what he had promised not to do;[and h]is daughter then did precisely what the confidentiality agreement was designed to prevent, advertising to the [school] community that [her father] had been successful in his age discrimination and retaliation case against the school") <www.3dca.flcourts.org/Opinions/3D13-1952.rh.pdf>. *See also* Matthew Stucker, *Girl costs father $80,000 with 'SUCK IT' Facebook post*, CNN (Mar. 14, 2014) <http://www.cnn.com/2014/03/02/us/facebook-post-costs-father/>.

[31] Jason Bartolone, *Shirtless Photos of State Rep. Peter Nehr Cause a Stir*, Dunedin Patch (July 27, 2012) <dunedin.patch.com/groups/politics-and-elections/p/shirtless-photos-of-state-rep-peter-nehr-cause-a-stir-976391f9>.

[32] Sunde Farquhar, *State Rep. District 65: Nehr Loses to Zimmermann*, Palm Harbor Patch (Nov. 7, 2012) <palmharbor.patch.com/groups/politics-and-elections/p/election-night-state-rep-district-65-race>.

[33] Proskauer Rose LLP, Social Media in the Workplace Around the World 3.0; 2013/14 Survey, at 2 (.pdf p. 4) (June 24, 2014) ("[f]or the first time since conducting this survey, the majority of businesses have had to deal with social media misuse[; m]oreover, more than 70% of businesses reported having to take disciplinary action against employees for misuse") <www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf>.

- FINRA broker standards;
- the Securities and Exchange Commission's ("SEC's") Division of Investment Management's 2014 Guidances for publicly traded companies[34] and for investment advisers, respectively;[35] and
- the Federal Drug Administration's ("FDA's") Office of Prescription Drug Promotion's ("OPDP's") 2014 draft Guidances as to social-media advertising as to prescription-drugs and medical devices.[36]

In Spring 2013, the Federal Trade Commission ("FTC") had promulgated more social-media related guidance[37] Remember that FTC regulations, including as to endorsements/testimonials, apply to all companies affecting interstate commerce, not just publicly traded ones – and not just companies in highly regulated industries.

In addition, in January 2013, the Federal Financial Institutions Examination Council (FFIEC) had entered the fray by "releas[ing] proposed guidance on the applicability of

---

[34] SEC, Securities Act Rules § 110, Rule 134, Questions 110.1 and 110.2 (promulgated Apr. 21, 2014) <http://www.sec.gov/divisions/corpfin/guidance/securitiesactrules-interps.htm>, as discussed in Joe Mont, *To Tweet or Not to Tweet? The SEC Has Some New Guidance*, Compliance Week (Apr. 23, 2014) <http://www.complianceweek.com/to-tweet-or-not-to-tweet-the-sec-has-some-new-guidance/article/343935/>.

[35] SEC, Investment Management <www.sec.gov/investment> (last visited July 4, 2014), linking to Guidance Update No. 2014-14, *GUIDANCE ON THE TESTIMONIAL RULE AND SOCIAL MEDIA* (Mar. 28, 2014, as modified June 6, 2014) <www.sec.gov/investment/im-guidance-2014-04.pdf >. *See also* Joe Mont, *Friended on Facebook? Praised on Yelp? The SEC May Take a Look*, Compliance Week (Apr. 3, 2014) <http://www.complianceweek.com/friended-on-facebook-praised-on-yelp-the-sec-may-take-a-look/article/341229/>.

[36] *See* FDA Center for Drug Evaluation and Research ("CDER") (last visited July 4, 2014) <www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm397791.htm>, linking to these two items as to "Prescription Drugs and Medical Devices": *Internet/Social Media Platforms with Character Space Limitations— Presenting Risk and Benefit Information* (June 13, 2014) <www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM401087.pdf>; and *Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation* (June 13, 2014) <www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM401079.pdf>. *See also* Victoria Loughery, *FDA Issues Draft Guidance Docs On How To Provide Accurate Risk/Benefit Info in 140 Characters Or Less And Clean Up 3rd Party UGC [129/140]* , Proskauer on Advertising Law (June 23, 2014) <http://tinyurl.com/Proskauer-6-23-14>; By Ginny Boland, *FDA Internet and Social Media Guidances Issued Today*¸ FDA Life (June 17, 2014) <http://www.fdalife.com/2014/06/17/fda-internet-and-social-media-guidances-issued-today/>. *Compare* William A. Ruskin, *Pharmaceutical Failure to Warn.... On Facebook?* LexisNexis Legal Newsroom (Mar. 19, 2014) <http://tinyurl.com/Ruskin-FDA-3-19-14> (discussing HHS FDA warning letter NDA #02194 TIROSINT (Feb. 28, 2014) <http://tinyurl.com/FDA-Tirosint-2-28-14>)).

[37] *See* FTC Staff Revises Online Advertising Disclosure Guidelines (Mar. 12, 2013) <http://www.ftc.gov/opa/2013/03/dotcom.shtm>, which is additional to the testimonials regulations found at 16 C.F.R. Part 255 <ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr255_main_02.tpl>. *See also FTC Approves Final Order Settling Charges That Public Relations Firm Used Misleading Online Endorsements to Market Gaming Apps*, FTC (Nov. 26, 2010) <ftc.gov/opa/2010/11/reverb.shtm>; *FTC Pursues Online Endorsements by Undisclosed Insiders*, F&W Lit. Alert (Sep. 2, 2010) <http://www.fenwick.com/publications/Pages/Litigation-Alert-The-FTC-Pursues-Online-Endorsements-by-Undisclosed-Insiders.aspx>.

consumer protection and compliance laws, regulations, and policies to activities conducted via social media by banks, savings associations, and credit unions, as well as nonbank entities supervised by the Consumer Financial Protection Bureau and state regulators."[38] The FFIEC's "final guidance" was released in December 2013.[39]

The Web 2.0 world (arguably now Web 3.0 !) of user-generated content (UGC), including employees' respective individual home pages on social networking sites and ill-advised tweets on Twitter, have begun to extend traditional legal concepts into new contexts Throughout the ensuing (sub-)sections of this Paper (and when reviewing the samples linked from the list that is **Item # 1 of Appendix A**), please interpret each reference to "blog" to encompass all of the many and varied ways any given individual can become a publisher in our modern world. As to whether and to what extent an employer can regulate employees' speech on their own social-media pages without being successfully accused of having committed a National Labor Relations Act (NLRA) unfair labor practice, *see* Section V(B)(3) below.

(ii) CDA Immunity Occasionally

Employee misuse of the internet is still rife with potential respondeat superior or negligent supervision liability for employers. Nonetheless, every once in a while a reported decision grants an employer immunity as an "interactive computer service" ("ICS") under the federal Communications Decency Act ("CDA").[40] Below is a summary of the two pro-employer decisions in this convoluted area of case law,[41] followed by a list of caveats and cites to countervailing decisions.

One such decision, *Miller v. Federal Express Corp.*,[42] is ambiguous as to whether the person who posted one of the three underlying allegedly defamatory

---

[38] FFIEC, *Financial Regulators Propose Guidance on Social Media*, Press Release (Jan. 22, 2013) <www.ffiec.gov/press/pr012213.htm>.

[39] FFIEC, *Financial Regulators Issue Final Guidance on Social Media*, Release (Dec. 11, 2013) <ffiec.gov/press/pr121113.htm> (linking to FFIEC, *Social Media: Consumer Compliance Risk Mgmt. Guidance*, (Dec. 2013) <http://www.ffiec.gov/press/Doc/FFIEC%20Social%20Media%20Guidance.doc>). *See generally* Poindexter, et al., *FFIEC Issues Final Guidance on Social Media Usage by Financial Institutions*, SociallyAware (Jan. 7, 2014) <www.sociallyawareblog.com/2014/01/07/ffiec-issues-final-guidance-on-social-media-usage-by-financial-institutions/>; Joe Mont, *Banks Get Needed Advice For Navigating Social Media Dangers*, Compliance Week (Dec. 12, 2013) <complianceweek.com/banks-get-needed-advice-for-navigating-social-media-dangers/article/325302>.

[40] 47 U.S.C.A. § 230 <www.gpo.gov/fdsys/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm>. As to the CDA generally, *see* Robert D. Brownstone, et al., 9 *Data Security & Privacy Law,* Privacy Litig. Ch. §§ 9:153 through 9:158 (West 2015); Robert Brownstone and Chad Woodford, *Web Sites' CDA § 230 Immunity: An Ever-Expanding Universe?* ALJ LJN., Vol. 1, No. 2 (Mar. 2006) <www.fenwick.com/news/documents/dec06privacy_website.pdf >.

[41] For an excellent short analysis of this area, *see* Eric Goldman, *Employer Gets Section 230 Immunity For Employee's Posts–Miller v. FedEx*, Tech. & Marketing Law Blog (Apr. 4, 2014) <webcache.googleusercontent.com/search?q=cache:http://blog.ericgoldman.org/archives/2014/04/employer-gets-section-230-immunity-for-employees-posts-miller-v-fedex.htm&strip=1>

[42] *Miller v. Federal Express Corp.*, 6 N.E. 3d 1006 (Ind. Ct. App. April 3, 2014) <http://www.in.gov/judiciary/opinions/pdf/04031401pdm.pdf>.

statements was an employee or a customer of one of the two corporate Defendants.[43] However, as to the other Defendant, it was definitive that the poster of the other two comments *was* an employee – in fact "the vice president of corporate sponsorship."[44] In *Miller* an Indiana appellate court found CDA immunity for *both* corporate defendants because the defamation Complaint had treated them as the actual publishers of the pertinent statements rather than alleging respondeat superior liability for the actions of others.[45]

Miller relied on the other pro-employer decision on this issue, namely one from a California appellate court *Delfino v. Agilent Technologies, Inc.*,[46] back in 2006. In that case, a third party filed a lawsuit against Agilent alleging that the Company was liable for threatening emails and electronic postings generated at Yahoo.com by an Agilent employee while he was using the company's internet connection. The cyberthreats were sent via the employee's own Yahoo! webmail account and posted on a Yahoo! Message board. The two causes of action were for intentional and negligent infliction of emotional distress.

The court concluded that the employee's actions were "plainly outside the scope of his employment" and noted that the employee was acting "out of personal malice." The court emphasized that Agilent was unaware of the employee's actions until it was contacted by the FBI, and that the company fully cooperated once it became aware of the situation. The court also noted that the employee was terminated a week after confessing that he had in fact sent at least one of the threatening messages while logged into Agilent's network.

In finding for Agilent, the appeals court held that the Company was a provider of computer services and not a publisher or speaker of information for purposes of the CDA.[47] Thus, the company was immune because its internet connection was the mere conduit for the employee, who authored the offensive emails and postings.[48] The appeals court observed that, even if the company were not immune, Agilent would not be liable because there was no evidence that it had been aware of the employee's behavior.[49]

Moreover, the company had acted promptly once it learned that the employee was using company computers to make the threats.[50] The appeals court suggested

---

[43] Goldman, supra note 41.

[44] 6 N.E. 3d at 1018.

[45] 6 N.E. 3d at 1010.

[46] *Delfino v. Agilent Technologies, Inc.*, 145 Cal. App. 4th 790, 52 Cal. Rptr. 3d 376 (Cal. App. 6 Dist. Dec. 14, 2006) <http://caselaw.findlaw.com/data2/californiastatecases/H028993.PDF>.

[47] *Id.* at 805-06.

[48] *Id.* at 807.

[49] *Id.* at 817.

[50] *Id.* at 811.

that imposing liability on employers for employee misuse of company computers could have a "chilling effect" on free speech because it could motive employers to use "extreme employer oversight of employee activities" to protect themselves from liability.[51] The court added that such a burden could be "enormous" for employers.[52]

While those two decisions are somewhat promising for employers, there are many reasons why it would be risky to rely on the existence of CDA immunity. The caveats include:

- Indiana's or California's view of the CDA may not carry the day in other states, let alone in the federal courts. Indeed the *Miller* / *Delfino* view has been rejected and or distinguished by an Illinois state appellate court[53], a California appellate court (in an unpublished opinion)[54] and also a federal district court within the Sixth Circuit.[55]

- A key fact in *Delfino* for respondeat superior purposes was that the employee was neither using the employer's own e-mail system nor communicating as to work-related content.

- A cyberthreat, as occurred in *Delfino*, is just one concern an employer should have about employee internet usage – as evidenced by the various topics discussed throughout the entirety of Section I(B) of this paper.

---

[51] *Id.* at 816.

[52] *Id.*

[53] *Lansing v. Southwest Airlines*, 980 N.E. 2d 630, 641, 366 Ill. Dec. 537 (Ill. App. 1 Dist. June 8, 2012) ("[§230](c)(1) of the CDA limits who may be called the publisher of information that appears online, and plaintiff's negligent supervision cause of action does not depend on who published [the employee's offensive information[; c]onsequently ... the CDA does not bar plaintiff's cause of action") <state.il.us/court/Opinions/AppellateCourt/2012/1stDistrict/1101164.pdf>, *appeal denied*, 979 N.E.2d 878 (Ill. Sep. 26, 2012), available at .pdf p. 51 at <state.il.us/court/SupremeCourt/PLA_Ann/2012/092612.pdf>. *Lansing* rejected the *Delfino* holding, distinguishing it on multiple bases, including the following:

> In *Delfino*, the court's analysis of the scope of immunity under section 230(c)(1) was primarily confined to the context of the plaintiffs' intentional and negligent infliction of emotional distress claims, which were similar to claims for defamation and did seek to hold the defendant liable for conduct derived from the publication of the offensive information. Accordingly, *Delfino*'s conclusion that the CDA's immunity bars a negligent supervision claim lacks analysis and is not persuasive.

Id. at 640.

[54] *Espinoza v. County of Orange*, 2012 WL 420149 (Cal. App. 4 Dist. Feb. 9, 2012) (unpublished) <http://www.leagle.com/decision/In%20CACO%2020120209057> .

[55] *Avery v. Idelaire Technologies Corp.*, 2007 WL 1574269 (E.D. Tenn. May 29, 2007) (in hostile environment case, denying part of Defendant-employers' summary judgment motion; "the Court is not aware of any federal case in the country that has applied the [CDA] in such a manner, and the Court declines to do so now") <www.steptoe.com/assets/attachments/3039.pdf>.

- The way the Complaint styles the relevant cause(s) of action seems to greatly impact the potential for Defendant to successfully invoke CDA immunity.

On different facts, a significant predicate for CDA immunity – namely no evidence that the employer played any role in the creation or development of the messages – might be lacking. In that scenario, two other theories could still proceed: respondeat superior and negligent supervision.

C. Public Sector

Public sector employers bear additional risks to those described above as to the private sector. Those risks keep growing in due to the ever-increasing use of – and rewards from – social media for government agencies, municipalities, legislators, legislatures' committees and the like.[56] Moreover, evidence of problematic communications may live on long-term in light of retention requirements found in many states' public records and/or open government laws.

For some public employees, social media activity presents unique problems; for example, judges using social media – and thus all attorneys who might consider connecting with judges in that realm -- should be aware of special considerations.[57]

Some state statutes and school district rules have imposed guidelines to ban private conversations between teachers and students on social media sites or via email. Some such rules have exceptions if a parent is part of the dialogue. These new regulatory rules are based on a concern about "boundary-crossing relationships with students."[58]

---

[56] *See, e.g.,* Carla Marinnucci, *@NeelKashkari campaigns 140 characters at a time*, S.F. Chronicle (Feb. 7, 2014) <www.sfgate.com/politics/article/NeelKashkari-campaigns-140-characters-at-a-time-5212351.php>; USA.gov, *Verify U.S. Federal Government Social Media Accounts* (Nov. 13, 2013) <www.usa.gov/Contact/verify-social-media.shtml>; CIO Council, Privacy Best Practices for Social Media, CIO Council (July 23, 2013) ("Federal Gov't 2.0") <https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf>.

[57] For a thorough compilation of resources on this issue, see the linked-to **Bibliography** listed as **Item # 5 of Appendix A** (including varying **ethics** advisory opinions in different states as to **judges**, **jurors** and – more broadly – **attorneys**). *See generally* additional public-records resources available from the author.

[58] Jennifer Preston, *Rules to Stop Pupil and Teacher From Getting Too Social Online*, N.Y. Times (Dec. 17, 2011) <http://www.nytimes.com/2011/12/18/business/media/rules-to-limit-how-teachers-and-students-interact-online.html>.

TIP: One approach when updating a TAUP to address social-networking sites is to cover these topics:

SOCIAL-NETWORKING SITES, WIKIS AND BLOGS – EMPLOYER-SPONSORED & PERSONAL

_. ***General Guidelines***

_. ***Specific Guidelines***

_. ***Employer-Sponsored Social-Networking Pages, Wikis, Blogs, etc.***

_. ***Personal Social-Networking Pages, Wikis, Blogs, etc.***

---

ii. eDiscovery of Social-Media Postings – and of Other Information in Employment Litigation

A. Expanded Discoverability

Electronic discovery ("eDiscovery") pertaining to emails and electronic documents has been commonplace in litigation for decades. Often, a Plaintiff's/employee's social-media postings, may end up being beneficial to employers. Indeed, in litigation, loose-lipped postings might be a discovery gold-mine for a Defendant/employer. Thus, over the past few years, posts, tweets, texts and "private" Facebook and MySpace messages have become entrenched, *court-endorsed* targets of production requests and subpoenas.[59]

Consequently, the volume of social media eDiscovery decisions in employment (and other) cases continues to grow, as indicated by the length of the linked **Bibliography** that is listed as **Item # 3 of Appendix A**. More and more of those decisions have made clear that "no principled reason to articulate different standards for the discoverability of communications through email, text message, or social media platforms."[60]

B. Social-Media as Probative of Emotional Distress – Case-law Split

However, there is a split in the case law to date as to whether the presence and/or lack of pertinent contemporaneous postings is relevant to a defense against an employee's claims of

---

[59] For an up-to-date set of links and summaries as to social-media eDiscovery decisions in employment and non-employment cases as well pertinent articles, *see* this Bibliography <tinyurl.com/SocialMediaeDiscoLatestFWLPP>, which is also **Item # 3 of Appendix A** to this Paper.

[60] *E.E.O.C. v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 432 (S.D. Ind. May 11, 2010) <web.archive.org/web/20110604063509/http:/www.ediscoverylaw.com/uploads/file/Simply%20Storage.pdf>.

emotional distress, *e.g.*, in harassment cases. Some courts have approved discoverability of social-media postings, including "communications [that] did not reference the events described in plaintiffs' complaint." [61] Other courts have not been willing to cut such a broad swath.

C. Preservation/Spoliation, including as to BYOD

The key eDiscovery issue of preservation has come to the forefront in a number of judicial decisions and/or ethics opinions in the social-media context.[62] At least several employment decisions have found that a Plaintiff/employee had committed spoliation by respectively: deleting Facebook posts and photos;[63] and deactivating or deleting a Facebook account[64]

Preservation and production concerns also have arisen in various types of cases in the Bring Your Own Device ("BYOD") and personal-webmail contexts, in which the "possession, custody or control standard is very much in flux.[65] Some courts have expanded an entity litigant's duties to encompass an individual employee's smartphone

---

[61] *Robinson v. Jones Lag LaSalle Americas, Inc.*, 2012 WL 3763545, * (D. Ore. Aug. 29, 2012) (in race discrimination and retaliation case, granting in part motion to compel production of email, text and social-media communications relating to, *inter alia,* emotional distress) <http://docs.justia.com/cases/federal/district-courts/oregon/ordce/3:2012cv00127/105802/32/0.pdf>.

Compare Simply Storage, 270 F.R.D. at 435 ("severe emotional or mental injury [could] manifest itself in some SNS content, and an examination . . . might reveal whether onset occurred, when, and the degree of distress]; further, information that evidences other stressors . . . is also relevant") <web.archive.org/web/20110604063509/http://www.ediscoverylaw.com/uploads/file/Simply%20Storage.pdf> with *Giacchetto v. Patchogue-Medford Union Free School Dist.*, 293 F.R.D. 112 (E.D.N.Y. May 6, 2013) ("Plaintiff's routine status updates and/or communications on social networking websites are not, as a general matter, relevant to her claim for emotional distress damages, nor are such . . . likely to lead to . . . admissible evidence regarding the same[; t]he Court does find, however, find that certain limited social networking postings should be produced") <web.archive.org/web/20130822061802/http://www.employerlawreport.com/uploads/file/Giachetto.pdf> and *Mailhoit v. Home Depot USA Inc. et al.*, 2012 WL 3939063, 116 Fair Empl. Prac. (BNA) 265, 83 Fed. R. Serv. 3d 585 (C.D. Cal. Sept. 7, 2012) (in gender and disability discrimination case, denying all three aspects of motion to compel that related to emotional distress) <scholar.google.com/scholar_case?case=17855446275012887254&hl=en&as_sdt=2006>.

[62] *See also* **Slides 24-27 of Appendix B**.

[63] *See, e.g., Painter v. Atwood*, 2014 WL 1089694 (D. Nev. Mar. 18, 2014) <http://www.aceds.org/wp-content/uploads/2014/04/213888337-Painter-v-Atwood.pdf>.

[64] *See, e.g., Crowe v. Marquette Transp.*, 2015 U.S. Dist. LEXIS 9198 (E.D. La. 1/20/15) (deactivation rather than permanent deletion) <www.gpo.gov/fdsys/pkg/USCOURTS-laed-2_14-cv-01130/pdf/USCOURTS-laed-2_14-cv-01130-0.pdf>; *Chapman v. Hiland Operating, LLC*, 2014 WL 2434775 (D. N.D. May 29, 2014) <docs.justia.com/cases/federal/district-courts/north-dakota/nddce/1:2013cv00052/26738/172/0.pdf>, as discussed in Joshua Gilliland, *A Measured Response to Social Media Preservation*, Bow Tie Law's Blog (June 17, 2014) <bowtielaw.wordpress.com/2014/06/17/a-measured-response-to-social-media-preservation>.

[65] Mark F. Foley, *Employer E-Discovery Duties Expand in a "BYOD" Environment Re: Employee Devices,* WTN News (Feb, 7, 2014) <http://www.vonbriesen.com/our-services/practice-areas/536/technology-law/articles/article-detail/2289/employer-e-discovery-duties-expand-in-a-byod-environment>

texts, IM's and/or personal webmail accounts.[66] However, other courts have gone in the opposite direction.[67] For an interesting discussion of how BYOD issues can come to roost downstream in electronic discovery, *see* Rebekah Mintzer, *'Deflategate' Lessons for E-Discovery Device Policies*, Corp. Counsel (5/18/15) (quoting throughout the author of this white paper) <www.corpcounsel.com/home/id=1202726599927/>. As to some tips on proactive policy formulation in this regard, *see* Section V(B)(2) below.

D. Authentication, *e.g.*, at Trial

Some decisions and articles have also addressed the issue of the authentication of social media content. *See* the cited/linked resources in the linked **Bibliography** that is listed as **Item # 3 of Appendix A**.

PRACTICAL TIP: The author has been using a powerful program, X1 Social Discovery <http://www.x1.com/products/x1_social_discovery>. That tool captures from the internet – and ostensibly authenticates[68] – publicly available electronic evidence from, among other sources, social-media sites such as Twitter, Facebook and LinkedIn. The X1 Social Discovery software program, in the course of being able to capture a given public tweet, records and maintains detailed authenticating information as to that tweet, in dozens of categories.[69]

---

[66] *See, e.g., Small v. Univ. Med. Ctr. of S. Nev.*, 2014 WL 4079507 (D. Nev. Aug. 18, 2014) (Special Master's lengthy Report), available at <https://cases.justia.com/federal/district-courts/nevada/nvdce/2:2013cv00298/92919/189/0.pdf>; *In re Pradaxa Prods. Liab. Litig.*, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013) <http://www.aceds.org/wp-content/uploads/2014/01/In-Re-Pradaxa-12-9-13-Opinion-.pdf>, *rescinded on other grounds*. 745 F.3d 216 (7th Cir. Jan. 24, 2014) <http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2014/D01-24/C:13-3898:J:Posner:aut:T:fnOp:N:1279508:S:0>; *Puerto Rico Telephone v. San Juan Cable*, 2013 WL 5533711 D. P.R. Oct. 7, 2013) (in antritrust case, denying without prejudice motion for sanctions but finding spoliation because company's preservation duty extended to personal email accounts of three managing officers where company presumably knew they had used those accounts to run company business for seven years) <justia.com/cases/federal/district-courts/puerto-rico/prdce/3:2011cv02135/91114/196/0.pdf>; *See also* Gareth Evans, *Perils of E-Discovery Reflected in Sanctions Opinion*, Law Tech. News (Dec. 23, 2013) ("U.S.D.C. Judge David Herndon issues a blistering 51-page opinion imposing nearly $1 million in punitive sanctions on the defendants in . . . Pradaxa") <gibsondunn.com/publications/Documents/EvansPerilsofEDiscovery.pdf>.

[67] *See, e.g., Cotton v. Costco Wholesale Corp.*, 2013 WL 381997, *6 (.pdf p. 10) (D. Kan. July 24, 2013) (in harassment/discrimination case , denying motion to compel as to texts sent from personal smartphones) <http://www.gpo.gov/fdsys/pkg/USCOURTS-ksd-2_12-cv-02731/pdf/USCOURTS-ksd-2_12-cv-02731-0.pdf>.

[68] John Patzakis, Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence (Mar. 31, 2014) <www.x1.com/download/X1Discovery_whitepaper_Social_Media.pdf>.

[69] Mark Lanterman, *"Elephant in the Room" – Case Studies of Social Media in Civil and Criminal Cases*, X1 next generation eDISCOVERY Law & Tech Blog (June 10, 2014) (guest blogger, CTO of Computer Forensics Services, Inc., noting that "in a recent intellectual property theft suit, I used X1 to collect the publicly available LinkedIn profile of a disgruntled employee, who left her company for a competitor") <http://blog.x1discovery.com/2014/06/10/elephant-in-the-room-case-studies-of-social-media-in-civil-and-criminal-cases/>.

Those categories of "data about data" – a/k/a "metadata" – include exact web address ("link"), time of original posting to the second, time of collection from the public web, "MD5 hash"[70] and multiple other items. Even the mainstream media has now gotten wise to the fact that "In a Single [140- character] Tweet, as Many Pieces of Metadata as There Are Characters."[71]

X1 Social Discovery can also collect and authenticate – hopefully the trial judge's satisfaction -- the contents of, for example, a Gmail box or a Yahoo mailbox provided the login credentials not only are available but have also been legally obtained (*see* ECPA issue mentioned in **Section IIB)(1) below**. For other tools/platforms, *see* **Slide 20 of Appendix B**.

---

3. Prospective Employees' (Applicants') Internet Activity

As discussed in detail in **Section III(B)** below, job applicants may very well have left a trail on the Internet as to their personal lives – and even negative comments as to jobs for which they are applying. Even if such content is not still live, it may live on via the Wayback Machine, a/k/a, the Internet Archive <archive.org/index.php>[72]

Someday soon, all public tweets on Twitter will be readily searchable in a National Archives database to be maintained by the Library of Congress. Moreover, public records obligations may very well require state and local governmental entities to archive and retain tweets and other posts that individuals may have placed on governmental social media pages.

According to a 2013 poll of" more than 2,000 hiring managers and human resources (HR) employees . . . 37 percent of the companies surveyed used social networking sites to prescreen candidates, . . . 11 percent said they planned to start doing so in the future [and o]nly 15 percent of companies had policies prohibiting the practice."[73] Note also that universities and colleges apparently typically pay attention to high-school-ers' social media posts when deciding whom to admit.[74]

---

[70] An "MD5 hash" is a unique multi-character string assigned algorithmically to each item of electronic information, functioning as an electronic "fingerprint" to demonstrate authenticity and chain of custody. *See, e.g., Definition: MD5* <searchsecurity.techtarget.com/definition/MD5> (Sep. 2005).

[71] Elizabeth Dwoskin, In a Single Tweet, as Many Pieces of Metadata as There Are Characters, Wall St. J. (June 6, 2014) <http://blogs.wsj.com/digits/2014/06/06/in-a-single-tweet-as-many-pieces-of-metadata-as-there-are-characters/tab/print/>.

[72] To learn more about use and admissibility of Internet Archive evidence, *see* Gregory P. Joseph, *Judicial Notice of Internet Evidence*, 82 USLW Case Alert & Legal News No. 34, at 10 n. 67 (Mar. 11, 2014) <jha.com/us/filemanager/judicial_notice_of_internet_evidence.pdf>; James L. Quarles III and Richard A. Crudo, *[Way]Back to the Future: Using the Wayback Machine in Patent Litigation*, 6 Landslide No. 3, ABA (Feb. 24, 2014) <americanbar.org/publications/landslide/2013-14/january-february/wayback_the_future.html>.

[73] Warne S. Heath, *Web-Surfing Your Job Applicants—TMI?* Mondaq (Jan. 28, 2014) <http://www.mondaq.com/unitedstates/x/288968/>.

[74] Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, N.Y. Times (Nov. 9. 2013) <nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html?pagewanted=all>

One concern employers should keep in mind is that their online research of applicants can have negative legal consequences, for example, if they uncover information that could support a disparate impact discrimination claim.

II. MONITORING OF EMPLOYEES' ELECTRONIC ACTIVITIES

A. Introduction

Courts have generally upheld employer interests in monitoring the use of their computer systems, including employer-provided email and Internet connections. While the case law recognizes an employer's right to monitor employee use of the company network, traditional labor and employment law can restrict the employer's ability to act upon that information in formulating employment decisions. Each employer needs to decide its most apt place on the spectrum from lenient to strict while it strives to create and maintain a defensible regime.[75]

B. Legality – Some Justifications and Some Countervailing Concerns

Some of the legal justifications for monitoring include these three statutory schemes: the Federal Electronic Communications Privacy Act ("ECPA"); state analogues to the ECPA; and the federal Computer Fraud and Abuse Act ("CFAA"). Two of the potential legal constrictions on monitoring are: labor laws such as the National Labor Relations Act (NLRA); and invasion of privacy claims under state constitutional law and/or case law.

1. Federal Electronic Communications Privacy Act (ECPA) and similar common-law and constitutional law claims

a. ECPA (Wiretap & SCA) Limits on Intrusions, Including into Workers' Private Email Accounts

As to employer-provided e-mail systems, many courts follow an expansive view of the "provider" exception of 18 U.S.C. § 2701(c). Those decisions have upheld an employer's right to retrieve and read such e-mails. Note, though, that viable claims for violations of the Stored Communications Act (SCA) – Title II of the ECPA – *have* been found in the different contexts of an employer's accessing an employee's private website and an employee's private e-mail account, respectively. However, one 2013 decision found that a co-worker – a Facebook "friend" of Plaintiff – was authorized to share screenshots of her posts with management such that the employer had not violated the SCA.[76]

---

[75] *See generally* Steve Lohr, *Unblinking Eyes Track Employees Workplace Surveillance Sees Good and Bad*, N.Y. Times (June 21, 2014) <www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html>; Nancy Flynn and Lewis Maltby, *Should Companies Monitor Their Employees' Social Media?* Wall St. J. (May 11, 2014) <http://online.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685>, linking to authors' debate/podcast at <http://podcast.mktw.net/wsj/audio/20140512/pod-wsjwndebatepodcast1/pod-wsjwndebatepodcast1.mp3> (subscription required for article but apparently not for podcast).

[76] *Ehling v. Monmouth-Ocean Hospital Service Corp.,* 2013 WL 4436539 (D.N.J. Aug. 20, 2013) (although SCA's protections extended to non-public Facebook wall posts, SCA's "authorized use" exception applied) <https://docs.google.com/file/d/0B7_eyMD-sepNRDRpTHNUVFVqTlk/edit?usp=sharing&pli=1>.

Many employees avoid using corporate e-mail systems to send "private" messages, but will use their work computers to access web-based e-mail services such as Gmail and Yahoo mail Many of these employees may not realize that such activity leaves electronic footprints on the hard drives of company-issued computers. Nor are many employees likely aware that commercially available software allows employers to monitor, keystroke by keystroke, the text they type into these pages.

If there is no actual trail left on an employer's system or computer, then, under federal case law (and even per an occasional state court opinion applying the ECPA) , an employer should not go as far as to actually log into and/or access an (ex-)employee's personal webmail account or a password-protected social-media group page. Doing so is a crime under the ECPA as well as potentially leading to civil liability (and punitive damages) too.

As to an employer's legal searches of its own systems (and perhaps also employees' (company-issued or not?) local machines), the importance of having an explicit pertinent policy in place – establishing the right to monitor and inspect – was buttressed by the U.S. Supreme Court in *City of Ontario v. Quon*.[77] Although a Fourth Amendment decision,[78] *Quon* has had implications in other contexts. *See* the ensuing sub-section (d)(i) for some details.

Two years ago, *Lazette v. Kulmatycki*, 2013 WL 2455937 (N.D. Ohio June 5, 2013) <http://www.gpo.gov/fdsys/pkg/USCOURTS-ohnd-3_12-cv-02416/pdf/USCOURTS-ohnd-3_12-cv-02416-0.pdf> became an example of a "how-not-to" when a supervisor secretly read 48,000 personal GMail account messages of an employee who had separated from the company 18 months previously -- via her returned company-issued Blackberry. The court deemed a Gmail server to be the requisite ECPA "facility" and thus denied a motion to dismiss an SCA claim – but not a Wiretap claim.[79] In addition, in a 2014 case, an employee's SCA claim survived summary judgment where she claimed it had inaptly – without authorization -- accessed, and posted via, her social media accounts while she was out on medical leave. *Maremont v. Susan Fredman Design Group, Ltd.*, 2014 WL 812401 (N.D. Ill. Mar. 3, 2014) <digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1653&context=historical>.

Yet, in an even more recent case, a different (pro-employer) result was reached where the fault lay with the former employee for enabling the former employer to gain access to his text messages. *Sunbelt Rentals v. Victor*, 2014 WL 4274313 (N.D. Cal. Aug. 28, 2014) <cases.justia.com/federal/district-courts/california/candce/4:2013cv04240/269981/58/0.pdf>. *Compare Rajaee v. Design Tech Homes*, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014) <http://leagle.com/decision/In%20FDCO%2020141113H36/RAJAEE%20v.%20DESIGN%20TECH%

[77] *Ontario v. Quon*, 560 U.S. 746 (U.S. June 17, 2010) <supremecourt.gov/opinions/09pdf/08-1332.pdf>.

[78] The SCA part of the Ninth Circuit's decision is anomalous and, in any event, was not taken up on certiorari by the U.S. Supreme Court.

[79] *But see Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. Dec. 12, 2012) (SCA *not* violated by unauthorized access to data stored on personal cell phone, which was not a "facility") <http://www.ca5.uscourts.gov/opinions/pub/11/11-41118-CV0.wpd.pdf>. *See generally* Jon Hyman, *Who owns personal email on an employer-issued smartphone?* Ohio Employer's Law Blog (July 17, 2013) <http://www.ohioemployerlawblog.com/2013/07/who-owns-personal-email-on-employer.html?goback=%2Egde_3921974_member_259091140>; Rory McNamara, *Court Ruling Impacts BYOD*, IAPP Privacy Tracker (July 9, 2013) <http://www.privacyassociation.org/privacy_tracker/post/court_ruling_impacts_byod>.

20HOMES,%20LTD> (dismissing CFAA and SCA claims where employer had remote-wiped device of former employee). An excellent analysis of many of the ECPA decisions discussed in this Section is in Mark H. Moore, *Workplace Disputes Under the Stored Communications Act*, Corporate Counsel (Oct. 20, 2014) <corpcounsel.com/id=1202673764306/Workplace-Disputes-Under-the-Stored-Communications-Act>.

In general, there is a lot of confusion in the case law under the ECPA, in light of Congress' failure to act to bring the statutory provisions in line with modern technologies.[80] Moreover, the issues get even more complicated when foreign citizens' electronic communications and/or overseas repositories are in question. Indeed there have been seemingly irreconcilable results in a couple SCA cases involving subpoenas served on Microsoft.[81]

One key point: In the social-media setting is that, when dealing with social media posts, an attempt should first be made to get the poster to disclose on his/her own or to consent to some discovery directly.[82] *See also* **Slide 21 of Appendix B** as to Facebook's "Download Your Information" and Twitter's "Your Twitter Archive."

b. Common-law, Including as to Attorney-Client Privilege

In the social-media realm, the analysis of whether a person has a reasonable expectation of privacy for purposes of a common-law invasion of privacy claim is context-dependent. For example, courts may be more likely to find a reasonable expectation of privacy where Facebook posts are restricted[83] or where emails were viewed on a computer designated for personal use.[84] In general, to avoid any arguments premised on a

---

[80] *See generally* <http://www.digitaldueprocess.org>.

[81] *Compare In re Warrant to Search a Certain Email Account Controlled and Maintained By Microsoft Corp.*, 1:13-mj-02814 (S.D.N.Y. Apr. 25, 2014) (in context of search warrant as to emails stored in Ireland, ruling that "[e]ven when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law") <pdfserver.amlaw.com/nlj/microsoft-warrant-sdny.pdf> with *Suzlon Energy Ltd. v. Sridhar [Microsoft]*, 671 F.3d 726 9th Cir. Oct. 3, 2011) (in non-employer-employee case, SCA protected foreign citizen's emails stored in U.S. in Microsoft's Hotmail environment) <ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf>.

[82] *See generally* A. Louis Dorny, *Get Consent and Avoid Sanctions*, Cal. Lawyer (July 2012) <callawyer.com/clstory.cfm?eid=923324>.

[83] *Ehling v. Monmouth-Ocean Hospital Service Corp.,* Civ. No. 2:11-CV 033305 (WJM) (D.N.J. May 30, 2012) (denying motion to dismiss common-law invasion claim because of fact question whether non-profit employee's restriction of access to her Facebook page gave her a reasonable expectation of privacy) <docs.justia.com/cases/federal/district-courts/new-jersey/njdce/2:2011cv03305/260497/23/0.pdf?1338465179>. *See also Ehling v. Monmouth-Ocean Hospital Service Corp.,* 2013 WL 4436539 (D.N.J. Aug. 20, 2013) (although the SCA's protections extended to non-public Facebook wall posts, by virtue of being a "friend" of Plaintiff, co-worker was "authorized" to make screenshots and share them with management) <https://docs.google.com/file/d/0B7_eyMD-sepNRDRpTHNUVFVqTlk/edit?usp=sharing>.

[84] *Doe v. City of San Francisco,* No. C10-04700 THE (N.D. Cal. June 12, 2012) (denying defendant's motion for judgment as matter of law as to SCA and common-law invasion claims; as to latter, reasoning that municipal employee had reasonable expectation of privacy in web-based emails viewed from a shared workplace computer designated for personal use by employees) <docs.justia.com/cases/federal/district-courts/california/candce/3:2010cv04700/233056/220/0.pdf>.

"reasonable expectation of privacy," in their policies on Internet and e-mail use employers may want to emphasize that communications sent through third-party e mail services are equally subject to monitoring.

Note, though, that, at times, an employer's reliance on a strong Technology Acceptable Use Policy ("TAUP") – especially its No-Employee-Expectation-of-Privacy ("NoEEP") provision -- have been trumped by attorney-client privilege. In those scenarios, policy language and enforcement practices have not been airtight and thus were deemed to give way to public-policy favoring protection of privilege. The outcomes in these types of clashes continue to diverge – with several decisions over the past few years rejecting in whole or in part an (ex-) employee's arguments that attorney-client privilege trumped a no-expectation-of-privacy policy.

As many of the various privilege-vs.-TAUP decisions as the author could find – some hinging on factual circumstances and others on public-policy -- are gathered in the **Bibliography** that is listed as **Item # 4 of Appendix A**.

PRACTICAL TIP: Employers should seriously consider establishing an investigation manual that, among other protocols, red-flags an ostensibly privileged communication as a sensitive issue that an incident-response team should run up the flagpole to the employer's legal counsel.

c. Constitutional Limits

i. 4th-Amendment (*Riley* and *Quon* Lessons for ALL Employers (public and private sectors)

A. Smartphone Searches – After Seizures

In June 2014, the U.S. Supreme Court unanimously upheld individuals' Fourth Amendment privacy rights in their cell phones' contents when such a device is seized by an arresting officer. *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473 (June 25, 2014) <http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>. While some of the consequences of *Riley* seem clear, many other ramifications of that decision will need to play out over time.[85] For the employer/employee context, two takeaways seem quite significant:

- 1) The Court notes that Defendants in *Riley* had "concede[d] that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant."[86] Thus, employers need to be aware – and remind their employees – that, upon, arrest, a cell phone and all its contents will likely automatically be in police custody.

[85] *See generally* Tyler G. Newby, *Supreme Court Defends Expectation of Privacy In Cell Phone Data*, Fenwick & West Lit. Alert (June 26, 2014) <fenwick.com/publications/Pages/Litigation-Alert-Supreme-Court-Defends-Expectation-of-Privacy-In-Cell-Phone-Data.aspx>.

[86] *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473, 2486 (pdf p.12) (June 25, 2014) <http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>.

- 2) Nothing in *Riley* expressly indicates any diminishment of and employer's rights to *its own data* stored either:

    - a) on *its own systems*, *see, e.g., Liebeskind v. Rutgers Univ.*, 2014 WL 7662032, 2015 Fair Empl. Prac. Cas. (BNA) 174,886, 2015 IER Cases ¶174,886 (N.J. Super. Ct. App. Div. Jan. 22, 2015) (unpublished opinion rejecting Fourth Amendment and common law invasion claims as to state university's extraction of employee's internet browsing activity in light of broad, clear TAUP) <http://www.njlawarchive.com/archive/a0544-12.pdf>; or

    - b) on devices owned by employees. Nonetheless, the Court's ringing endorsement of privacy in the vast data contents of a personal smartphone implicitly sends a message to all employers that they may want to be extremely clear in their policies and training when restricting or eliminating expectations of privacy.

That second takeaway – keep your TAUP and related training up-to-date and clear – had been the express lesson in the 2010 U.S. Supreme Court decision in *Quon*.[87] In *Quon,* a police officer brought SCA, Fourth Amendment and California constitutional claims against a wireless company and his employer (the City of Ontario) for allegedly violating his privacy by respectively accessing, divulging and reviewing the contents of his personal text messages transmitted by way of an *employer-provided* pager.[88] After many years of litigation, the U.S. Supreme Court ultimately found that the employee did not have a reasonable expectation of privacy under the Fourth Amendment even though a manager had made ill-advised comments to the contrary and even though the pertinent TAUP was out of date.

The author's "Top Ten" post-*Quon* tips for a compliant TAUP for a public or private employer are available in multiple places online.[89] The first two takeaways on that list relate to the Bring Your Own Device (BYOD) issue, which has become more and more complicated in recent years. *See* **Section V(B)(2) below**.

B. Employees' Whereabouts and Posts

Of note as to tracking employees' whereabouts is the startling 2013 Fourth Amendment decision in *Cunningham v. N.Y.S. State DOL*, 21 N.Y.3d 515, 997 N.E.2d 468 (June 27, 2013) <http://www.nycourts.gov/ctapps/Decisions/2013/Jun13/123opn13-Decision.pdf>. There, New York's highest court found that a public employer did not violate the Fourth Amendment when,

---

[87] *Ontario v. Quon*, 560 U.S. 746 (U.S. June 17, 2010) <supremecourt.gov/opinions/09pdf/08-1332.pdf>.

[88] For a full discussion of *Quon*, *see* Brownstone eWorkplace II page 1 supra, at 20-24 (.pdf pp. 25-29) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>.

[89] *Id.* at 23-24 (.pdf pp. 28-29) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>.; Robert D. Brownstone, *Employers' Technology Acceptable Use Policies — Top Ten Tips*, IT Law Today (Aug. 13, 2013) <www.itlawtoday.com/2013/08/drafting-technology-acceptable-use-policies-top-ten-tips/>.

without seeking a warrant, it attached a GPS device to the personal car of an employee/ administrator whom it was investigating for alleged false time reports. The *Cunningham* majority found the GPS surveillance unreasonable only because it occurred 24/7 "without making a reasonable effort to avoid tracking [the] employee outside of business hours." *Id.* The author doubts this scary decision will start a trend,[90] because a handbook policy staking out such a right would be difficult to defend, even for a private sector employer.[91] Even if valid on its face, the inevitable targeted enforcement of such an approach would be highly susceptible to a claim of discrimination and/or arbitrariness.

As to Fourth Amendment issues regarding tweets, *see Rosario v. Clark County School District*, 2013 WL 3679375 (D. Nev. July 3, 2013) (["w]hen a person tweets on Twitter to his or her friends, that person takes the risk that the friend will turn the information over to the government") <http://docs.justia.com/cases/federal/district-courts/nevada/nvdce/2:2013cv00362/93113/26/0.pdf> (citing *U.S. v. Meregildo*, 883 F.Supp.2d 523, 525 (S.D.N.Y. Aug. 10, 2012) (for Fourth Amendment purposes, no reasonable expectation of privacy in Facebook profile, to which Government received access via "use of a cooperating witness who was one of [Defendant]'s Facebook 'friends'") <http://www.x1.com/download/US_v_Meregildo.pdf>)).[92]

ii. First Amendment

Case law in the area of the First Amendment generally favors the right to communicate freely. This tendency is especially pronounced when the speech is of a controversial and thought-provoking nature. However, in the employment setting, courts tend to enforce clear computer usage policies that prohibit conduct such as sending discriminatory or harassing communications. Thus, employers, particularly government entities, must walk a fine line between enforcing their anti-harassment and computer usage policies, while remaining cognizant of their employees' free speech rights.

Many reported First Amendment decisions in the employment setting tackle whether a police officer was acting in the capacity of a public employee or private

---

[90] *Compare United States v. Jones*, 132 S. Ct. 945, 181 L. Ed.2d 911 (2012) ("attachment of a Global–Positioning–System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitute[d] a search or seizure within the meaning of the Fourth Amendment") with <supremecourt.gov/opinions/11pdf/10-1259.pdf>; *Carniol v. NYC TLC*, 42 Misc. 3d 199, 975 N.Y.S .2d 842 (N.Y. Cty. Sup. Sep. 26, 2013) (placement was not surreptitious; "even if petitioner could show that he has a legitimate expectation of privacy in trip data gathered by the GPS device, which he cannot, his fourth amendment claim of privacy would be outweighed by the legitimate governmental interests") <law.justia.com/cases/new-york/other-courts/2013/2013-ny-slip-op-23358.html>.

[91] *See* Pete Brush, *NY Court Plants Supreme Court Seed With GPS Snoop Ruling*, Law360 (July 2, 2013) ("'I find it hard to believe that a public sector employer could write a policy saying, "We have the right to attach a device to your car," [Robert] Brownstone said.") <leclairryan.com/files/Uploads/Documents/GPS%20Snoop%20Ruling_Law360.pdf>.

[92] *See also* Molly DiBianca, *Is There a Reasonable Expectation of Privacy In Your Tweets?* Delaware Employment Law Blog (July 23, 2013) <delawareemploymentlawblog.com/2013/07/is-there-a-reasonable-expectation-of-privacy-in-your-tweets.html>.

citizen. Some others involve have involved a teacher or a professor.[93] On the one hand, some public sector employees – such as teachers and police – are often subject to stricter codes of conduct than private sector employees. On the other hand, the First Amendment can be on the employee's side in certain situations.

In any event, for a number of years First Amendment implications have arisen from employee use of employer-provided email systems. Not surprisingly this decade has seen growth in the number of those types of First Amendment decisions involving posts on Facebook or another social media site. In that arena, a new issue entails whether "liking" a Facebook page is protected speech. In a 2013 decision, the Fourth Circuit held that:

> "[l]iking a political candidate's campaign page communicates the user's approval of the candidate and supports the campaign by associating the user with it. In this way, it is the Internet equivalent of displaying a political sign in one's front yard, which the Supreme Court has held is substantive speech (citation omitted).[94]

In a state such as California, which has a constitutional right to *privacy*, private sector employees may have a tenable constitutional *privacy* claim. However, as to constitutional *free speech rights*, typically private sector employers are immune from First Amendment claims.[95]

2. State Analogues to the ECPA and to Federal Constitutional Provisions

Since the federal constitution and the federal ECPA do not preempt the field of

---

[93] *In re O'Brien*, 2013 WL 132508 (N.J. Super. A.D. Jan. 11, 2013) (upholding removal of elementary school teacher from tenured position based on Facebook posts including "I'm not a teacher—I'm a warden for future criminals!") <www.njlawarchive.com/archive/a2452-11.pdf >*; Van Heerden v. Bd. of Supervisors of LSU*, 2011 WL 5008410 (M.D. La. Oct. 20, 2011) (First Amendment claim *not* barred where public university professor's statement not made in capacity as public employee, but rather made as private citizen) <http://www.aaup.org/NR/rdonlyres/CA20F70D-71D6-45D3-972F-AA3F3FB390A0/0/VanHeerden_v_LSU_102011.pdf>. *See also Dahlia v. Rodriguez,* 735 F.3d 1060 (9th Cir. Aug. 21, 2013) (reversal of lower court's dismissal of § 1983 case brought by police officer who disclosed fellow officers' conduct) <cdn.ca9.uscourts.gov/datastore/opinions/2013/08/21/10-55978.pdf>. To keep abreast of First Amendment decisions in the employer-employee context, *see generally* Molly DiBianca, Public Sector, Delaware Employment Law Blog (last visited Mar. 1, 2015) <http://www.delawareemploymentlawblog.com/public-sector/>.

[94] *Bland v. Roberts*, 730 F.3d 368 (4th Cir. 2013) <ca4.uscourts.gov/Opinions/Published/121671.P.pdf>, *reversing* 857 F.Supp.2d 599 (E.D. Va. Apr. 24, 2012) ("merely 'liking' a Facebook page is insufficient speech to merit constitutional protection[;] cases where courts have found that constitutional speech protections extended to Facebook posts, actual statements existed within the record") <tinyurl.com/Bland-Roberts-EDVa>.

[95] *See, e.g., Barnett v. Aultman Hosp*., 2012 WL 5378738, *9 (N.D. Ohio Oct. 31, 2012) (granting summary judgment for employer on FMLA claim and other claims premised on alleged retaliation for Facebook message; holding that "absent state action, a wrongful discharge tort claim cannot be based upon the public policy expressed in the First Amendment to the federal constitution") <gpo.gov/fdsys/pkg/USCOURTS-ohnd-5_11-cv-00399/pdf/USCOURTS-ohnd-5_11-cv-00399-1.pdf>.

monitoring of electronic communications, several states have enacted more stringent restrictions regarding the interception of wire and electronic communications. Among those states are California (*see* individual right of privacy in Cal. Const. Art. 1 §1) and New Jersey.

As discussed in **Section III(B)(3)** below, many states have passed or are currently considering legislation that would prohibit employers from asking employees for social media passwords,[96] and others have enacted more comprehensive privacy legislation.[97] One analyst notes that state privacy legislation that "protect[s] the social media privacy rights of employees . . . may also protect . . . employers from frivolous social media related lawsuits."[98] That same analyst expressed the view that California AB 1844:

> is a huge win for the business community because it may provide California businesses with a legal liability shield from plaintiffs who may allege that businesses have a legal duty to monitor their employees' personal password protected digital content. This legislation may collectively save California businesses tens of millions of dollars a year in costs to monitor their employees' personal digital accounts. In addition, this law may save California businesses tens of millions of dollars per year on cyber liability insurance premiums that would accompany a duty to monitor employees in the digital/social media space.

To protect against statutory and constitutional (as well as common-law) invasion claims for invasion of privacy, many employers decrease their employees' expectations of privacy in e-mail by giving written notice to employees that monitoring regularly takes place – and by avoiding policies or customs that might justify an employee's expectation of privacy.

Note that, as discussed in more detail in **Sections II(B)(4) and V(B)(3)** below, open issues remain – as to all employers impacting interstate commerce – under the National Labor Relations Act as to the extent to which an employer may:

- prohibit non-business uses of its e-mail system and network; and
- monitor employee use of e-mail systems and other environments not owned by the employer, *e.g.,* employee use of webmail accounts and personal social-media pages via a work-provided Internet connection.

Future interpretation of the NLRA – especially by a federal circuit court – in various factual contexts could also have ripple effects in other federal and state arenas, whether or not union issues are involved.

---

[96] *See, e.g.,* Md. Ann. Code § 3-712 <http://tinyurl.com/Md-3-712>. *See generally* the 2015, 204, 2013 and 2012 legislation gathered in National Conference of State Legislators ("NCSL"), *Employer Access to Social Media Usernames and Passwords* <www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx>.

[97] Bradley Shear, *California is the First State to Enact Comprehensive Social Media Privacy Legislation*, Shear on Social Media Law (Sept. 27, 2012) (discussing CA SB 1349 and AB 1844) <http://www.shearsocialmedia.com/2012/09/california-is-first-state-to-enact.html>.

[98] *Id.*

3. Computer Fraud and Abuse Act ("CFAA")

a. Introduction

Employers victimized by disloyal employees who have misappropriated sensitive computer data and/or sabotaged their employer's computer systems on the way out the door have successfully found recourse under the civil remedy provision of the Computer Fraud and Abuse Act ("CFAA"). If found viable by the judge, such a claim confers federal subject matter jurisdiction, enabling the suit to proceed in federal court.

As noted in predecessor versions of this White Paper, a federal CFAA claim may be a desirable supplement to a state law trade secret action against a disloyal former employee who accessed proprietary information before separating from a company. Moreover, depending on the underlying facts as to the accessed information, a CFAA claim may be an alternative/replacement cause of action – and thus a very attractive option – where the complained-of conduct may not satisfy all the elements of a trade secret misappropriation claim. A trade secret cause of action requires that misappropriated information be confidential and well-guarded. However, as discussed in detail in the predecessor versions of this sub-section, there is a split in case law as to the viability of the CFAA's application in cases based on allegations of trade secret misappropriation by a former employee. *See also* this piece, which addresses these same points: Nicholas A. Sarokhanian and Victor D. Vital, Corporate Counsel, *Using the CFAA to Stop Data From Walking Out the Door*, Corp. Counsel (Nov. 6, 2014) <http://www.corpcounsel.com/id=1202673805434/Using-the-CFAA-to-Stop-Data-From-Walking-Out-the-Door>.

Generally, in addition to criminalizing various categories of offending conduct, the CFAA permits injured parties to sue for economic damages and injunctive relief for two types of improper computer access: prohibited access by someone without any pertinent authorization; and access exceeding the scope of authorization.[99] The CFAA, in 18 U.S.C. § 1030, enables "[a]ny person who suffers damage or loss by reason of a violation . . . [to] . . . maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Employers face two hurdles in establishing their CFAA claims: alleging the requisite lack of authorized access; and stating a valid claim for statutorily defined damage and/or loss.

b. "Authorized Access" – Split in Authority on Key Theory

Currently still on the cutting edge is whether a disloyal employee is an apt defendant on a CFAA cause of action brought by his/her (former) employer. There continue to be Circuit court opinions and dozens of U.S. district court decisions in this area. The holdings – and thus the outcomes – in those decisions have split roughly evenly.

In the typical factual scenario in these cases, the offending employee had permission to use the company computer in the course of his or her duties. Thus, while still employed at the company, he or she arguably had "authorized" access to the proprietary material at issue.

---

[99] The Computer Fraud & Abuse Act ("CFAA") prohibits, among other things: "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and . . . obtain[ing] anything of value," 18 U.S.C. § 1030(a)(4). *See generally* Robert D. Brownstone, et al., 9 *Data Security & Privacy Law,* Privacy Litig. Ch. §§ 9:3 through 9:19 (West 2015).

One decision following that view quoted a commentator's "burglary" analogy as follows:

> If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter. Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 571 (2011).[100]

In response to an attack on a Complaint's sufficiency, Plaintiffs have routinely counter-argued that: "authorized access" extended only to job duties; and, once the employee downloaded information for nefarious purposes, the access became unauthorized. The author's colleague Sebastian Kaplan has charted out the case-law split on this "authorized access" issue as:

- Plaintiff (Employer)-Friendly: 1st, 5th, 6th, 7th, 8th & 11th;[101] and
- Plaintiff (Employer)-Hostile: 2nd, 3rd, 4th, 9th & 10th.[102]

[100] *Dresser-Rand Co. v. Jones*, 957 F. Supp.2d 610, 614 (E.D. Pa. July 23, 2013) <gpo.gov/fdsys/pkg/USCOURTS-paed-2_10-cv-02031/pdf/USCOURTS-paed-2_10-cv-02031-0.pdf>.

[101] Relatively recent decisions following this pro-employer view include: *Carnegie Strategic Design Eng'rs, LLC v. Cloherty*, 2014 WL 896636, W.D. Pa. March 6, 2014) (within Third Circuit) <http://www.ediscoverylawtoday.com/files/2014/03/Non-Compete-Opinion_Unauthorized-Access.pdf>; *Beta Tech., Inc. v. Meyers* 2013 WL 5602930 (S. D. Tex. Oct, 10, 2013) (within Eleventh Circuit) <docs.justia.com/cases/federal/district-courts/texas/txsdce/4:2013cv01282/1077500/29/0.pdf?1381586108>, discussed in Brandon Krajewski, *Can Your Company's Computer Use Policy Form the Basis for a Civil Claim?* Quarles & Brady Trade Secrets Law Update (Oct. 29, 2013) <http://www.quarles.com/publications/can-your-companys-computer-use-policy-form-the-basis-for-a-civil-claim/>; *Custom Hardware Engineering & Consulting, Inc. v. Dowell*, 918 F. Supp. 2d 916 (E.D. Mo. January 23, 2013) (within Eighth Circuit) <docs.justia.com/cases/federal/district-courts/missouri/moedce/4:2010cv00653/106055/354/0.pdf>. *Compare NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816 (N.D. Cal. May 12, 2014) (author's firm is counsel of record for Nimble) <https://cases.justia.com/federal/district-courts/california/candce/5:2013cv05058/271449/66/0.pdf?ts=1399968756> (citing *Weingand v. Harland Financial Solutions, Inc.*, 2012 WL 2327660 (access by a *former* employee whose credentials still functioned could support CFAA claim) (N.D. Cal. June 19, 2012) <http://www.tradesecretslaw.com/files/2012/08/Weingand.pdf>).

c. Loss/Damage Requirement

The second hurdle to bringing a viable action against a current or former employee is proving loss and/or damage. Most courts are now holding that "loss" cannot consist merely of lost trade secrets or related lost revenue, but must comprise costs that flow directly from the computer-access event, such as costs caused by interruption of service. However, other district courts interpret "loss" broadly, reading "any reasonable cost" in a manner that includes any cognizable injury to the complaining party. *See, e.g., Network Cargo Systems International, Inc. v. Pappas*, 2014 WL 1674650, *3 (N.D. Ill. Apr. 25, 2014) (denying motion to dismiss CFAA claim based on deleting data) <http://www.gpo.gov/fdsys/pkg/USCOURTS-ilnd-1_13-cv-09171/pdf/USCOURTS-ilnd-1_13-cv-09171-0.pdf>.

Several of the CFAA theories proffered by employers involve proving statutory "damage," which can be a tough row to hoe when data is simply accessed and copied, but not in any way impaired. Courts vary widely on what comprises "damage." The majority of courts nationwide have found that trade secret misappropriation alone does not meet the statutory definition of damage, in that the Act's use of the word "integrity" to define damage requires "some diminution in the completeness or usability of data or information on a computer system."

Similarly, a 2014 decision failed to find "loss" based on investigation costs – for "damage assessment and mitigation" -- in a case against a former employee who had forwarded many emails containing confidential customer information to his personal email account, in violation of company policy.[103]

---

[102] Relatively recent decisions following this pro-employee view include: *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. Apr. 10, 2012) (*en banc*) <ca9.uscourts.gov/datastore/opinions/2011/11/02/10-10038o.pdf>; *Enki Corp. v. Freedman*, 2014 WL 261798 (N.D. Cal. Jan. 23, 2014) (within Ninth Circuit) <docs.justia.com/cases/federal/district-courts/california/candce/5:2013cv02201/266206/44/0.pdf>, as discussed in Daniel J. McCoy and Dan Ko Obuhanych, *Access Of Computer System With Log-In Credentials Is Not Unlawful "Hacking,"* Fenwick & West EMP. Brief (Feb. 2014) <fenwick.com/publications/Pages/Fenwick-Employment-Brief-February-2014.aspx?WT.mc_id=EB_021814>; *Quad Knopf, Inc. v. S. Valley Bio. Consulting*, 2014 WL 1333999 *4 (E.D. Cal. Apr. 3, 2014) (dismissing CFAA claims where employees were "employed at the time of the alleged transmittal") <http://www.gpo.gov/fdsys/pkg/USCOURTS-caed-1_13-cv-01262/pdf/USCOURTS-caed-1_13-cv-01262-2.pdf>; *Integral Dev. Corp. v. Tolat*, 2013 WL 5781581 *4 (N.D. Cal. Oct. 25, 2013) (dismissing CFAA claims; "at the time of the alleged acquisition of the materials, Tolat was working for Integral") (within Ninth Circuit) <https://cases.justia.com/federal/district-courts/california/candce/3:2012cv06575/262043/185/0.pdf>; *Roadlink Workforce Solutions LLC v. Malpass*, 2013 WL 5274812 (W.D. Wash. Sep. 18, 2013) (within Ninth Circuit) <docs.justia.com/cases/federal/district-courts/washington/wawdce/3:2013cv05459/193451/16/0.pdf>; *Dresser-Rand Co. v. Jones*, 957 F. Supp.2d 610, 614 (E.D. Pa. July 23, 2013) <gpo.gov/fdsys/pkg/USCOURTS-paed-2_10-cv-02031/pdf/USCOURTS-paed-2_10-cv-02031-0.pdf> (within Third Circuit); *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514 (S.D.N.Y. Mar. 20, 2013) (within Second Circuit) <noncompetereport.com/files/2013/03/JBCHoldings-NY-LLC-v.-Pakter1.pdf>.

[103] *SBS Worldwide, Inc. v. Potts*, 2014 WL 499001 (N.D. Ill. Feb. 7, 2014) <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2013cv06557/287656/28/0.pdf>.

4. Countervailing Concern # 1 – Protected Union Activity Under the National Labor Relations Act, et al. ("NLRA")

Laws protecting union activity may hinder some attempts to restrict employee electronic communications.[104] In the past several years, the NLRB has begun to dig in deep on the parameters of protection of concerted activity in the 21st Century context. Late 2010 ushered in a new era of NLRB scrutiny – as to union and non-union workforces – as to social-media policies

In the past four years, there has been a flurry of additional NLRB activity in the social-media context as well as early this year in the email context. *See* **Section V(B)(3)** below for a discussion of this decade's developments and proceedings tackling whether employee posts constitute employment terms and/or conditions. Although the law is in flux and the NLRB has been coming down hard on employers, *e.g.*, NLRB, *Report of the General Counsel Concerning Employer Rules*, Memo No. GC 15-04 (Mar. 18, 2015) <http://apps.nlrb.gov/link/document.aspx/09031d4581b37135>, the author hopes that these three types of prohibitions could withstand even the NLRB's extreme views:

- 1) do not lie about the company or any of its executives or staff;
- 2) do not disclose outside of the company any of the company's proprietary information or intellectual property that is confidential unless duly authorized to do so or unless doing so is necessary for "two or more employees take action for their mutual aid or protection regarding terms and conditions of employment;"
- 3) on any personal social-media page on which you identify yourself in any way as an employee of the company, disclaim that you are speaking on behalf of the company.[105]

On the other side of the coin, employers should be cautious about disciplining employees for using the company e-mail system – as well as employees' own personal social-media pages – to engage in labor organizing or in other arguably protected activity – such as criticizing management, raising safety concerns or comparing compensation. Similarly, under federal and state civil rights anti-retaliation laws, communications critical of management may also be protected "opposition" if they relate to allegedly unlawful employment practices.

Either way, employers should also follow the typical best practices of: being as consistent as possible in applying such policies; and memorializing the in–the-trenches details as to the categories of communications they allow and disallow.

---

[104] For an overview of the pre-social-media law in this area, *see* Brownstone eWorkplace II, supra note 2, at 32-35 (.pdf pp. 37-40) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>.

[105] *See* this very short video: Robert D. Brownstone, *Two Key Elements Every Social Media Policy Should Include*, Fenwick & West LLP (Mar. 2013) <www.fenwick.com/Videos/Pages/Two-Key-Elements-Every-Social-Media-Policy-Should-Include.aspx>. For other drafting tips, *see* Sheeva J. Ghassemi-Vanni, Saundra Riley and Michael A. Sands, *Social Media Policies And The NLRB: What Employers Need To Know, JD Supra Business Advisor* (Mar. 4, 2013) <http://www.jdsupra.com/legalnews/social-media-policies-and-the-nlrb-what-84189/>.

5. Countervailing Concern # 2 – Avoiding Invasion of Privacy Claims[106]

Employers may wish to prevent misconduct by regularly monitoring their computer systems and network resources. However, to minimize the risk of employee privacy rights claims, an employer should implement an employee computer use policy that would enable it to monitor and search its computer network and systems at will.[107] Most decisions regarding the interception of a private employee's e-mail continue to find that no intrusion into the employee's privacy occurred. Yet, it is possible to construct some potentially viable theories of privacy violations.

The safest method to avoid liability under privacy laws is to achieve prior notice and consent.[108] Employers are wise to disseminate: (1) an employee computer use policy which, at a minimum, puts employees on notice of the full extent of the employer's rights to access electronically stored information. and (2) guidelines for employee use of e-mail, the internet and social-media.[109] *See* Section V below (and its counterpart in the cited predecessor White Paper) for further discussion of proactive policies.

III. INVESTIGATIONS AND BACKGROUND CHECKS

A. Credit Report Information Under FCRA, EEOC Guidelines and State-Analogues (and Criminal Background Checks)

To avoid the risk of a negligent hiring claim (and to hire the best employees), employers should diligently explore a candidate's background before extending an unconditional offer of employment. Consumer credit report information, as opposed to criminal history, is the major focus of this sub-section. It is worth noting first, though, that, in addition to state acts such as Massachusetts SB 2583passed in 2010,[110] municipalities have been entering the fray on background checks, *e.g.*:

- In June 2015, New York City enacted the "Fair Chance Act" Ordinance, amending Admin. Code § 8-107(10)-(11), effective as of September 27, 2015<nyc.gov/html/cchr/html/law/amendment_6_2015a.shtml> to provide various protections as summarized in Daniel J. McCoy and Saundra L.M. Riley, *New*

---

[106] *See generally* Brownstone eWorkplace II, supra note 2, at 35-36 (.pdf pp. 40-41) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pd>.

[107] *See, e.g.*, the samples linked off of the **Bibliography** that is **Item # 1 of Appendix A**.

[108] Anyone can escape liability under the ECPA if one of the parties to a communication consents to an interception or disclosure of a message. 18 U.S.C. § 2511(2)(d) and § 2702(b)(3).

[109] *See, e.g.*, the samples linked off of the **Bibliography** that is **Item # 1 of Appendix A**.

[110] CHAPTER 256 OF THE MASS. LAWS OF 2010, "*AN ACT REFORMING THE ADMINISTRATIVE PROCEDURES RELATIVE TO CRIMINAL OFFENDER RECORD INFORMATION AND PRE- AND POST-TRIAL SUPERVISED RELEASE* (see Senate No. 2583) Approved by the Governor, August 6, 2010" <http://www.malegislature.gov/Laws/SessionLaws/Acts/2010/Chapter256>.

York City Passes Ban-the-Box Ordinance, Fenwick Emp. Brief (June 22, 2015) <fenwick.com/publications/Pages/Fenwick-Employment-Brief---June-2015.aspx>

- In February 2014, the City and County of San Francisco passed an "[o]rdinance amending the Police Code to require employers and housing providers to limit the use of criminal history information, and follow certain procedures and restrictions when inquiring about and using conviction history information to make decisions about employment and tenancy in San Francisco."[111]

A must-read is the EEOC Guidance on the interplay of criminal background checks and alleged disparate impact under Title VII. EEOC, Enforcement Guidance No. 915.002, *Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964* (April 25, 2012) <eeoc.gov/laws/guidance/arrest_conviction.cfm>.[112] Two great sources are these compilations of slide decks: Devata, et al., *FCRA Class Actions in Employment on the Rise: Avoiding and Defending Claims*, Strafford Pubs. Webinar (Mar. 18, 2015) <http://media.straffordpub.com/products/fcra-class-actions-in-employment-on-the-rise-avoiding-and-defending-claims-2015-03-18/presentation.pdf>; Davis, et al., *Pre-Employment Background Screening: Latest Developments . . . Title VII, Fair Credit Reporting Act and State Laws*, Strafford Pubs. Webinar (July 2, 2013) <http://media.straffordpub.com/products/pre-employment-background-screening-latest-developments-2013-07-02/presentation.pdf>.[113]

In any event, as to credit report background checks, several types performed by outside investigators (termed "consumer reporting agencies" or "CRA's") are regulated by federal and state laws designed to protect consumer privacy and to ensure the accuracy of the records upon which the employer relies. Most notable among the pertinent statutory schemes is the federal Fair Credit Reporting Act ("FCRA").[114] The FCRA applies to private and public entities

[111] *See* Ordinance No. 131192 home page (Feb. 14, 2014) <http://tinyurl.com/Ord-131192-Home>, linking to the Ordinance itself <http://tinyurl.com/Ord-131192-Text>. *See also* Michael A. Sands and Sheeva J. Ghassemi-Vanni, San Francisco Limits Inquiry into Criminal History of Applicants and Employees, Fenwick & West Emp. Brief (Mar. 2014) <www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-March-2014.aspx?WT.mc_id=EB_031714>.

[112] The highlights are discussed in Fenwick & West, *EEOC Provides Guidance Regarding Use Of Criminal History In Employment Decisions*, Employment Brief (May 11, 2012) <http://www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-May-2012.aspx>.

[113] Among other items addressed therein are: Nat'l Emp. Law Project (NELP), *Ban the Box: Major U.S. Cities and Counties Adopt Fair Hiring Policies to Remove Unfair Barriers to Employment of People with Criminal Records* (April 2013) <nelp.3cdn.net/495bf1d813cadb030d_qxm6b9zbt.pdf>; *EEOC Files Suit Against Two Employers for Use of Criminal Background Checks*, Press Release (June 11, 2013) ("BMW Fired and Denied Hire to Class of Employees Who Worked Successfully for Years; Dollar General Disproportionately Excluded African Americans From Hire") <eeoc.gov/eeoc/newsroom/release/6-11-13.cfm>. *See also* the more recent slide decks compiled at Gordon and Konkel, *Avoiding Employer Liability Due to Employees' Expanded Privacy Rights: Crafting Effective Policies and Practices*, Strafford Pubs. Webinar (Mar. 19, 2014) <http://media.straffordpub.com/products/avoiding-employer-liability-due-to-employees-expanded-privacy-rights-crafting-effective-policies-and-practices-2014-03-19/presentation.pdf>.

[114] *See generally FTC Testifies on the Rights of Employees Under the Fair Credit Reporting Act* (Oct. 20, 2010) <http://www.ftc.gov/news-events/press-releases/2010/10/ftc-testifies-rights-employees-under-fair-credit-reporting-act >. The testimony itself is available at <web.archive.org/web/20130816181758/http://ftc.gov/os/testimony/101020eeoctestimony.pdf>.

alike. In that regard In March 2014, the EEOC published some new materials.[115] New challenges continue to emerge as to various types of references checks claimed to have run afoul of the FCRA. *See, e.g.*, *Sweet v. Linkedin*, No. 14-cv-04531 (N.D. Cal. Apr. 4, 2015) (dismissing class action based on LinkedIn Premium's "search for references" feature) <cases.justia.com/federal/district-courts/california/candce/5:2014cv04531/281365/33/0.pdf>.

Many states have analogous statutory schemes that are ostensibly stricter than the EEOC guidelines and/or than the FCRA. Those states are: California, Colorado, Connecticut, Delaware (legislation passed in 2014 as to public employers), Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont and Washington. *See* <ncsl.org/research/financial-services-and-commerce/use-of-credit-information-in-employment-2014-legislation.aspx>. New York City's analogous approach, *The Stop Credit Discrimination in Employment Act*, will become effective September 2. <legistar.council.nyc.gov/LegislationDetail.aspx?ID=1709692&GUID=61CC4810-E9ED-4F16-A765-FD1D190CEE6C>

B. Legality and Advisability of Following the Internet Trail

1. Overview

As to the brave new world of Web 2.0 and the quandary it creates for employers considering hiring a given applicant, some of the principles in this area seem to be as follows:

- Those who post information about themselves on the web without using protections to keep it from being publicly available will have an exceedingly weak "expectation of privacy" argument.
- An employer may lawfully search/Google as to an applicant as long as it does not take adverse actions based on a protected category.[116]
- As to the information an employer finds on a prospect's Web 2.0 page, the extent to which it can use the information is subject to traditional labor law concepts such as discrimination:
  - As in the "off-duty" context as to existing employees, an applicant's posts content demonstrating lack of ability to do, or interest in, the job, presumably the prospective employer may rely on it.
  - However, what if a hiring department only learns of a prospect's religion, race, gender, marital status and/or sexual preference from the individual's social-networking page?

[115] FTC, *Employment Background Checks: FTC, EEOC Offer Tips for Employers and Job Applicants* (Mar. 10, 2014) (linking to two brochures) <http://www.ftc.gov/news-events/press-releases/2014/03/employment-background-checks-ftc-eeoc-offer-tips-employers-job>.

[116] *See* Warne S. Heath, *Web-Surfing Your Job Applicants—TMI?* Mondaq (Jan. 28, 2014) <www.mondaq.com/unitedstates/x/288968/>, which makes a number of good points, including that:

> [A]n indiscrete HR staffer could fail to keep the information confidential and allow it to be known by coworkers, particularly if there is no clear policy on the issue. For example, learning that a new hire has a history of suing former employers could create suspicion among coworkers. Gossiping about the details of an applicant's religious practices could lead to a claim of discrimination and harassment.

Given the potential hazards of trying to parse – and, if challenged later, prove – what someone did and did not view and/or rely upon, an employer can take alternative approaches. On the one hand, an organization can develop, write up (and train on and do its best to follow) a realistic policy that allows lawful web-searching regarding prospects. It seems that many employers have gone that rout.[117] On the other hand, as some employers have publicly announced it is doing, an organization can decide to avoid web research altogether; and some commentators also echo that conservative approach.

2. Web Surfing/Searching as to Applicants

But, without a doubt, in some way, shape or form, *many* HR departments are now routinely web-surfing as to applicants. A new alternative is to rely on a third-party company to perform the social media background check.[118] The FTC has sent mixed signals as to the defensibility of that approach. In one instance in 2011, the FTC approved the potential legality of a start-up company, Social Intelligence™, <http://www.socialintel.com/>, which performs social-media background checks on applicants.[119] In 2012, though, the FTC issued warning letters to purveyors of mobile apps that purport to enable online background checks.[120]

Many a social media page contains information identifying the given individual's age, marital status, status as a parent, political views and/or religious views.[121] Indeed, websites, social media pages and associated apps intent to solicit, collect and gather such personal data.[122] So, what could go wrong? First, especially in the absence of a strict protocol, an HR staffer could fail to use discretion and discuss his/her findings – *e.g.*, an applicant's history of suing former employers – with multiple co-workers.

---

[117] *See Benny Evangelista Social media manners matter, job recruiters say*, S.F. Chronicle (Sep. 5, 2013) <http://www.sfgate.com/technology/article/Social-media-manners-matter-job-recruiters-say-4790675.php?pagewanted=all>.

[118] Presumably a provider with pertinent accreditation, *e.g.,* through the National Association of Professional Background Screeners ("NAPBS®") Accreditation Program <https://napbs.com/accreditation/index.cfm>.

[119] Brownstone eWorkplace II, page 1 supra, at 39 (.pdf p. 44), at footnotes 165-66.

[120] *FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act; Agency Sends Letter to Marketers of Six Apps for Background Screening*, Press Release (Feb. 7, 2012) (linking to three warning letters) <ftc.gov/opa/2012/02/mobileapps.shtm>. *See also* Fenwick & West LLP, *FTC: Marketers of Background Screening Mobile Applications May Be Consumer Reporting Agencies*, Emp. Brief (Feb. 15, 2012) <fenwick.com/publications/pages/fenwick-employment-brief-february-2012.aspx>.

[121] *See* Slide 37 (p. E-37; .pdf p. 108) of a prior version of these materials <itlawtoday.com/files/2013/06/eWorkplace_Materials_c_Brownstone_FWLLP_5-2-13.pdf>.

[122] *See, e.g.*, Julia Angwin and Jeremy Singer-Vine, *Selling You on Facebook*, Wall St. J. (Apr. 10, 2012) <http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html>.

Second, those involved in a hiring decision might actually document that a prospect's religious beliefs or the like impacted the ultimate decision not to choose that prospect.[123]

See also FTC, *The Fair Credit Reporting Act & social media: What businesses should know*, Bureau of Consumer Protection Business Center (June 23, 2011) (linking to other resources) <http://www.business.ftc.gov/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know>.

3. Seeking Full Transparency re: Applicants' Social-Media Pages?

An unresolved issue in this context is whether a prospective employer should be asking an applicant for his or her login and password information so the HR Department can *log in as the applicant*. Such a request overreaches, especially in the public sector context.[124] As to the private sector, a widespread similar practice has apparently developed. It goes by the name of "shoulder surfing," a/k/a having the applicant log in and surf his/her own Facebook or other social-media page while a staffer of the prospective employer watches. This type of forced-transparency practice has received a tremendous amount of press coverage, including as to Facebook's vehement objections.[125]

Moreover, at least 21 states have passed legislation banning employers from asking employees or job applicants for their login information to disclose a user name or password for a personal online account, such as social media credentials. Those states are Arkansas, Colorado, Connecticut (effective October 1, 2015), Illinois, Louisiana, Maryland, Michigan, Montana (effective April 23, 2015), Nevada, New Hampshire, New Mexico, New Jersey, Oklahoma, Oregon, Rhode Island, Tennessee (effective January 1, 2015), Utah, Vermont, Virginia (effective July 1, 2015), Wisconsin and Washington. Most of those expressly apply to state and local government units. At least 11 additional similar bills are pending as of mid-2015.[126] And at least eight of those states' laws also expressly or implicitly forbid shoulder-surfing.

---

[123] *See, e.g.,* the summary judgment denial and then settlement involving an astronomer believed to be a creationist based on writings on his public personal page in the religious discrimination case of *Gaskell v. Univ. of Ky.*, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010) <http://media.aclj.org/pdf/gaskell_summary_judgment_order_20101206.pdf>.

[124] *See* Abigail Rubinstein, 5 Questions Employers Shouldn't Ask Job Applicants, law360 (Nov. 30, 2012) <http://www.law360.com/articles/397482/5-questions-employers-shouldn-t-ask-job-applicants>.

[125] Martha C. White, *Can Interviewers Insist on 'Shoulder Surfing' Your Facebook Page?* Time (Mar. 9, 2012) <moneyland.time.com/2012/03/09/can-interviewers-insist-on-shoulder-surfing-your-facebook-page/>.

[126] *See generally* the 2012-2015 legislation gathered in National Conference of State Legislators ("NCSL"), *Employer Access to Social Media Usernames and Passwords* <www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx> (last updated July 9, 2015 and linking to links list for 21 states' laws at <ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx>). *See also* **Slides 47-48 in Appendix B**; **Section II(B)(2) above**; Robert D. Brownstone, *New Jersey 13th State to Protect Social Media Passwords*, ITLawToday (Aug. 29, 2013) <http://www.itlawtoday.com/2013/08/nj-13th-state-to-protect-employees-social-media-logins-passwords/>; Sarah O'Donohue, *'Like' it or Not, Password Protection Laws Could Protect Much More than Passwords*, 20 J. L. Bus. & Eth. (Aug. 1, 2013) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344801>.

4. Safekeeping of Background-Check Information

Once sensitive personal information has been legally gathered, the employer has duties to protect such information during the data's lifetime (*e.g.,* via encryption, as mentioned in **Section V(E) below**) and then to dispose of it securely when the information is no longer needed including per the FTC's Disposal Rule under FACTA).

IV. SEARCHING, SURVEILLING AND TRACKING PHYSICAL CONDUCT AND LOCATIONS

A. Workplace & Personal Searches

1. Workplace Searches

Employers may need to conduct physical searches of the workplace to prevent employee use or sale of drugs, to prevent theft, or simply to locate a file in an employee's desk. However, such searches – especially by public sector employers – may sometimes intrude into an employee's reasonable expectation of privacy.

The U.S. Supreme Court's 2014 *Riley* decision[127] assumed that officers' seizure of a cell phone incident to arrest is valid but it may have only done so given that the Defendants conceded that issue. But, in its main holding, *Riley* required a warrant for the authorities to access data stored on, let alone linked from, an individual's smartphone.

So, public sector employees may now argue that their employers need to tread more carefully in investigatory searches. As to *private* sector employers, presumably their inspection rights remain as extensive as staked out in the pertinent policies and training. More broadly, as to today's mobile workforce, public and private employers alike should be worried about work information being toted around by employees on personal devices. So, policies, protocols and training need to emphasize the dangers of local storage.

2. Personal Searches

Personal searches are more intrusive than work area searches and therefore can only be justified by an employer's strong showing of need. Employers should avoid conducting personal searches unless they can demonstrate justification based on circumstances pointing to a specific individual suspected of misconduct. Employers who anticipate the need to search individuals may mitigate their risk by providing advance notice of their policies.

---

[127] *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473 (June 25, 2014) <http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>. In light of *Riley*, it will be interesting to see what happens to precedent to the effect that a warrant is not – or may not be – required for the Government to obtain a court order under the SCA for an individual's "historical cell site" location data to be produced by a cell phone service provider. *See, e.g., In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. July 30, 2013) <http://www.ca5.uscourts.gov/opinions/pub/11/11-20884-CV0.wpd.pdf>. *See also* David Kravets, Cops Can Track Cellphones Without Warrants, Appeals Court Rules, Wired (July 30, 2013) <http://www.wired.com/threatlevel/2013/07/warrantless-cell-tracking/>.

B. Video Surveillance

Video surveillance may help deter employee misconduct, including theft and drug use. However, employers may still face constitutional or common law claims for invasion of privacy if they conduct video surveillance in areas where employees have a reasonable expectation of privacy. Moreover, states such as California have statutes outright prohibiting videotaping in certain locations. At a minimum, video surveillance should be disclosed. On the other side of the coin, a new concern revolves around employees who video themselves and then post an embarrassing-to-the-employer six-second video via Twitter's Vine app. *See* Jacob Gershman, *The Latest Social Media Concern for Employers*, Wall St. J. Law Blog (May 21, 2013) <blogs.wsj.com/law/2013/05/21/the-latest-social-media-concern-for-employers>.

C. Location Tracking – including RFID and GPS

The biggest legal development in this area is arguably last summer's startling decision by the majority – and warnings by the concurrence – in *Cunningham*,[128] discussed in Section II(B)(1)(c)(i)(B) above.

D. "Off-Duty" Activities

In spite of the broad frolic-and-detour monitoring approved by New York's highest court in *Cunningham*, there are typically reasons for employers to be more careful in that context and in various other ones touching on "off-duty" conduct. As discussed in Brownstone eWorkplace II, supra note 2, at 46-51 (.pdf pp. 51-56), off-duty conduct disputes most commonly arise in four areas: (1) competitive business activities; (2) substance use; (3) intimate relationships; (4) arrests and convictions; and (5) in today's Web-2.0/Social-networking world, many miscellaneous web activities.

1. Competitive Business Activities

For a relatively detailed discussion of this first area, *see* Robert D. Brownstone, *Workplace Privacy Policies* (Aug. 2009), at 56-57 (.pdf pp. 62-63) ("Brownstone eWorkplace I") <fenwick.com/docstore/publications/EIM/eWorkplace_Policies_Materials_Public_Sector_EEO_8-28-09.pdf>.

2. Substance Use

For this second area, *see id.* at 57 (.pdf p. 63). *See also City of Memphis Civil Service Com'n v. Payton*, 2012 WL 5422518 (Tenn. Ct. App. Nov. 07, 2012) (affirming firefighter's termination; positive drug screen results not subject to federal confidentiality rules) <tsc.state.tn.us/sites/default/files/paytonstevenopn.pdf>.

3. Dating and Intimate Relationships

For a relatively detailed 2009 discussion of this third area, *see id.* at 47-48 (.pdf pp. 52-53). For a new angle on this issue, take note of the 2011 U.S. Supreme Court decision in *Thompson v. North American Stainless, LP*, 131 S. Ct. 863, 178 L.Ed.2d 694 (2011)

---

[128] *Cunningham v. N.Y.S. State DOL*, 21 N.Y. 3d 515, 997 N.E. 2d 468 (June 27, 2013) <http://www.nycourts.gov/ctapps/Decisions/2013/Jun13/123opn13-Decision.pdf.

<http://www.supremecourt.gov/opinions/10pdf/09-291.pdf>. There, the Court upheld the viability of a Title VII claim brought by an ex-employee whose Complaint alleged that he had been fired several weeks after the employer learned that Plaintiff's fiancée/co-worker had filed a sex discrimination charge with the EEOC. *Id.* at 869-70.

For years, key developments have often focused on police or school teachers as to whom a code of conduct applied. Of course, when a case involves a teacher's alleged intimate relationship with a minor, many serious concerns are raised. But the legal standards are murkier as to the broader topic of online communications between a K-12 teacher and one of his/her students.

4. Arrests and Convictions[129]

Section III(A) above, as to pre-employment screening, is also applicable here to potential adverse action as to a current employee.[130] For a while, the current employees issue received a fair amount of press coverage in part due to the dog-fighting-ring-operation conviction, jail time, job-suspension and ultimate reinstatement of pro football player Michael Vick.

A jail sentence will cause an obvious work absence; but under those circumstances the employer can take the easier route of disciplining the employee for failure to report to work. Employers may likewise consider criminal activity implicating an employee's dishonesty, especially for jobs in industries such as financial services. However, as with other types of off-duty conduct, employers must consult the law of their jurisdiction before taking adverse employment action based on an employee's arrest or conviction.

5. Miscellaneous Web Activities

A 21st century employer has the potential to access a vast amount of publicly available information as to any given employee, especially if he/she is an avid Web 2.0 user. The EEOC held a meeting in March 2014 to address social-media in the workplace and published the testimony and a press release;[131] but it has not yet issued any formal guidance. As discussed above regarding prospects, well-thought out policies and consistent application thereof can greatly help an employer develop and demonstrate a legally defensible approach.

In a related issue, sometimes an employee challenges a post(s)-based firing as having been discriminately. Several of these cases have been sternly rejected by the courts, including in the FMLA setting. In 2012, there were at least two decisions rejecting FMLA claims, each of which had been premised on an

---

[129] *See generally* Brownstone eWorkplace II, supra note 2, at 49-50 (.pdf pp. 54-55) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>.

[130] *See also* L.M. Sixel, *How blanket employee screening policies can cause problems*, S.F. Chronicle (Jan. 24, 2014) <sfgate.com/business/article/How-blanket-employee-screening-policies-can-cause-5173668.php>.

[131] EEOC, *Social Media in the Workplace: Examining Implications for Equal Employment Opportunity Law* (Mar. 12, 2014) <http://www.eeoc.gov/eeoc/meetings/3-12-14/>.

employer's alleged improper reliance on one or more of an employee's Facebook posts.[132] Another similar dismissal followed in early 2013.[133]

A relatively new and unresolved issue relates to ownership of LinkedIn contacts ("connections") or of a Twitter handle/account or the like when an employee separates from the company. Some lawsuits have addressed whether such publicly available items can constitute trade secrets. In a new twist on this theme, a *current* employee – who was out on medical leave – was able to state a viable SCA claim against her employer for its allegedly inapt access of, and posting to, her Facebook and Twitter feeds. *Maremont v. Susan Fredman Design Group, Ltd.*, 2014 WL 812401 (N.D. Ill. Mar. 3, 2014) <digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1653&context=historical>. *See also* Mark H. Moore, *Workplace Disputes Under the Stored Communications Act*, Corporate Counsel (Oct. 20, 2014) <corpcounsel.com/id=1202673764306/Workplace-Disputes-Under-the-Stored-Communications-Act>.

Some of the ownership (*i.e.*, "eRolodex") lawsuits have addressed the related question of whether the widespread web availability of contact information can preclude organizations' customer lists from being protectable as trade secrets. In 2014, one California appellate decision found that this assessment entails a jury question. *Cellular Accessories For Less, Inc. v. Trinitas LLC*, 2014 WL 4627090 (C.D. Cal. Sep. 16, 2014) <https://cases.justia.com/federal/district-courts/california/cacdce/2:2012cv06736/539067/86/0.pdf>. That same decision also ruled the same way as to LinkedIn contacts. *Id.* For a detailed summary of this decision, *see* Dan McCoy and Dan Ko Obuhanych, *Are LinkedIn Contacts The Employer's Trade Secrets?* F&W Emp. Brief (Oct. 20, 2014) <http://www.fenwick.com/Publications/Pages/Fenwick-Employment-Brief---October-2014.aspx?WT.mc_id=EB_102014>. A related issue is whether a former employee's updating of her LinkedIn profile was "solicitation" of her prior employer's customers as to violate her noncompetition agreement.[134]

Moreover, executives, supervisors and managers at times recklessly take to the web to: fire an employee; explain the reasons for a termination; engage in a debate

---

[132] *Jaszczyszyn v. Advantage Health Physician Network*, 2012 WL 5416616, *1, *9 (6th Cir. Nov. 7, 2012) (affirming summary judgment for employer on interference and retaliation claims where employee had been "taking intermittent FMLA leave related to worsening pain from a back injury . . . [but] several of her coworkers saw pictures of her drinking at a local festival on Facebook and brought the matter up with their supervisor . . . [leading to] terminated her for fraud) <http://www.ca6.uscourts.gov/opinions.pdf/12a1152n-06.pdf>; *Barnett v. Aultman Hosp.*, 2012 WL 5378738, *9 (N.D. Ohio Oct. 31, 2012) (granting summary judgment for employer on FMLA claim and other claims premised on alleged retaliation for a Facebook message) <gpo.gov/fdsys/pkg/USCOURTS-ohnd-5_11-cv-00399/pdf/USCOURTS-ohnd-5_11-cv-00399-1.pdf>.

[133] *Lineberry v. Richards*, 2013 WL 438689, 20 Wage & Hour Cas.2d (BNA) 359 (E.D. Mich. Feb. 5, 2013) (leave abuse and dishonesty, as in *Barnett*) <http://www.gpo.gov/fdsys/pkg/USCOURTS-mied-2_11-cv-13752/pdf/USCOURTS-mied-2_11-cv-13752-0.pdf>.

[134] *KNF&T Staffing v. Muller*, No. 13-3676-BLS1 (Mass. Super. Ct. Suffolk Oct. 24, 2013) (rejecting employer's request for relief) <pdfserver.amlaw.com/nlj/MassSuperiorKNF&TvMullerPIOrder.pdf>. *See generally* Ken Shigley, *When Do Social Media Posts Violate Employees' Non-Solicitation Provisions?* Atlanta Injury Law Blog (Apr. 17, 2014) <atlantainjurylawblog.com/uncategorized/when-do-social-media-posts-violate-employees-non-solicitation-provisions.html>.

about whether an employee was disciplined too leniently or too severely; to announce one's own firing; or, once separating from the company, to air dirty laundry about supposed misconduct at the organization.

V. IMPLEMENTING LEGALLY-COMPLIANT AND DEFENSIBLE POLICIES

A. Introduction to Compliance

1. The Three E's – Establish, then Educate, then Enforce

Some identify the fundamental principles of policy implementation as "The Three E's," namely Establish, Educate and Enforce.[135] First, policy goals must be established. Second, once the policies are written, employees must be educated on the content. And, third, only then, should technology be used as one enforcement/ implementation mechanism – not as a magic-bullet. Employers who want to minimize risks associated with electronic communications and maximize employee compliance should start with well-crafted written rules and policies.[136]

2. Eliminating Employee Privacy Expectations – Notice, Reasonableness, etc.

Prophylactic agreements and policies can cut off future protracted litigation disputes. As evident in Sections I and II above, the many issues regarding electronic communications in the workplace continue to be defined and refined through legislation and litigation. Thus, legal issues regarding workplace electronic activity require careful, jurisdiction-specific analysis. There are two principles, however, that all employers should apply when considering acts which might arguably violate employee privacy: notice and reasonableness.

B. Some Key Privacy-Related Policies

1. Policies Eliminating Employee Privacy Expectations

a. Computer Systems and Hardware Policies

An effective use policy clearly sets forth that (1) network resources and computers (and other company-issued and company-supported electronic devices) are the property of the employer, and (2) the employees waive their privacy rights when they use these machines or devices. The scope should be broad, *e.g.,* that the Company owns "all information created, received or stored" on any "system, network, computer and mobile device provided or supported by the Company."[137] As discussed in Brownstone eWorkplace II, page 1 supra, at 52-53 (.pdf pp. 57-58) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-

---

[135] *See* Nancy Flynn, *The e-Policy HANDBOOK*, at Ch. 20 ("Employee Education Policies and Best Practices"), at 173 (2d ed. 2009) <tinyurl.com/3-Es-Flynn>, as quoted in Dunn, Darrell, *Email is Exhibit A*, Info. Week (May 8, 2006) <informationweek.com/e-mail-is-exhibit-a/d/d-id/1042925?print=yes>.

[136] For a podcast on this topic, listen to an interview of this White Paper's author at Jessica Liebrock, *Legal Current*, Thomson Reuters (Apr. 2012) <traffic.libsyn.com/legalcurrent/LegalCurrent_April2012.mp3>.

[137] *See, e.g.*, SAMPLES linked off of the list that is **Item # 1 of Appendix A**.

Media_Materials_NELI_Brownstone_4-3-12.pdf>, generic, vague log-on "banner" warnings as to "monitoring" may be insufficient but specific, clear policies can very effectively create "No Employee Expectation of Privacy" ("NoEEP").

In 2011, one state appellate court extended the NoEEP concept to an *employee's own computer* when that machine was physically in a workplace office and connected to the employer's network. *See Sitton v. Print Direction, Inc.*, 2011 WL 4669712 (Ga. App. Sep. 28, 2011) <http://caselaw.findlaw.com/ga-court-of-appeals/1594039.html>. The employer's inspection rights as to communications by an employee suspected of forming a competing venture even extended to readily viewable email messages in the employee's own personal webmail account. The reasons included that the:

> computer usage policy was not limited to [company]-owned equipment. The policy adverted to the necessity for the company 'to be able to respond to proper requests resulting from legal proceedings that call for electronically-stored evidence' and provided that for this reason, its employees should not regard 'electronic mail left on or transmitted over these systems' as 'private or confidential.' . . . . Even if the email was 'stored' elsewhere, the company's policy also stated that '[the company] will ... inspect the contents of computers, voice mail or electronic mail in the course of an investigation triggered by indications of unacceptable behavior.'

Id. at *3. Thus, the appellate court affirmed a judgment dismissing all of the employee's common law and state statutory privacy causes of action, the latter of which were brought under OCGA § 16-9-93(a)-(c) <http://law.justia.com/codes/georgia/2010/title-16/chapter-9/article-6/part-1/16-9-93/>. Note, though, that there may have been a different result under the federal ECPA.

The employer's overall right to inspect work-provided computers and portable-media that are physically in the office is typically much more straightforward; moreover, a physical lock on an employee's office door is typically of no consequence. *See* Brownstone eWorkplace II, page 1 supra, at 53 (.pdf pp. 58) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>. Moreover, in an employer/employee dispute, often the pertinent forensically recoverable information relates to the alleged theft and misuse of trade secrets and/or other proprietary information. In that setting, an ever-growing body of decisional law addresses a former employee's obligation to preserve the *status quo* so that the court and the former employer can follow the digital trail. *Id.* In addition, even in a garden-variety wrongful termination case, there may be preservation/spoliation issues. *Id.*

b. Inspection/Litigation Provisions[138]

Polices/agreements governing employees' use of employer-provided networks and computers can trump any ultimate employee arguments as to the reasonableness of a purported expectation of privacy. In this type of provision, it is wise to address not only Company Owned Personally Enabled (COPE) devices but also Bring Your Own Device ("BYOD"), as discussed in **Section V(B)(2) below**.

c. International Caveat[139]

Today's increasingly international economy requires American employers to pay close attention to privacy rules in other countries, which may be stringent indeed. For example, some data rules regulate the entire European Union (EU) region, some are country-specific, and some even apply at the province/state level. European rules tend to be much more protective of employees' privacy rights than United States law.

The pertinent limits placed on the search-and-discovery of foreign employees; personal data add to the employer considerations addressed throughout Section III of this White Paper. Significantly, the EU has taken the position that the transfer of employment records from European subsidiaries to their American parent companies must comply with the EU's Directive on Data Privacy.

The EU Commission is currently in the process of amending its Privacy Directive, likely to create more uniformity across the various EU countries. On the other side of the coin, however, throughout the world, including Asia and the South Pacific, different regulatory frameworks continue to emerge and evolve.

2. Special Issues Often Ignored: Voicemails / IM's / Smartphones / BYOD / Cloud[140]

Retention policies/protocols, computer use policies and other pertinent policies and protocols (such as when, or if, to erase hard drive data and network data of departing employees) need to be broad in scope. Their coverage should include voicemail, IM, text messages, smartphones, tablets and other company-issued mobile devices. Not only laptops but also other mobile devices – such as tablets (*e.g.*, iPads) and smartphones (*e.g.,* Androids and iPhones) – can retain sensitive materials that can be easily retrieved by hackers if data is not properly encrypted and/or not sufficiently "hard-wiped" before disposal of the device.

---

[138] *See* Brownstone eWorkplace II, page 1 supra, at 53-54 (.pdf pp. 58-59) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>.

[139] *See* Robert D. Brownstone, *Cross-Border eDiscovery* (Apr. 23, 1015) (lengthy slide deck) <http://www.itlawtoday.com/files/2015/04/Cross-Border-eDiscovery-ClearLaw-4-23-15-c-RBrownstone-FWLLP.pdf>; *see also* video of "eDiscovery 3.0" panel, Blackstone Discovery (Oct. 24, 2012) at <http://tinyurl.com/Blackstone-Video>.

[140] To learn more, *see* Brownstone eWorkplace II, supra note 2, at 54-55 (.pdf pp. 59-60) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf>.

A BYOD policy should be in place that addresses ownership, wiping, inspection and other issues as to employees' own devices. There are many options of how strict or lenient to be in this regard. From an eDiscovery perspective, stricter is better. Why? The employer ultimately may be deemed to have had possession, custody or control over BYOD devices – and, of course, Company-Owned-Personally-Enabled (COPE) device – for eDiscovery purposes.[141] Moreover, if there ends up being spoliation – or refusal to allow an inspection/collection – on behalf of the employee, then the employer can "throw him/her under the bus" and distance itself from such action.

From a cultural perspective at a given company, being too big-brotherish or too big-sisterish could be a problem. Organizations are deploying disparate various policy and technology approaches, including "containerization" to try to find a middle ground on the BYOD issue.[142] For information-security purposes, an employer should reserve the right to remote-wipe part (if possible) or all of the contents of a device. One recent decision upheld an employer's remote-wipe rights in the face of CFAA and ECPA claims that the court deemed not viable. *Rajaee v. Design Tech Homes*, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014) <leagle.com/decision/In%20FDCO%2020141113H36/RAJAEE%20v.%20DESIGN%20TECH%20HOMES,%20LTD>.

Whatever new or amended approach an employer takes as to BYOD, in light of the U.S. Supreme Court *Riley* decision, it may be wise to remind employees that, as opposed to arresting officers, employers in large part get to control access rights to employees' smartphones.

In addition, in recent years a new wave of devices, called "Wearables", has made the scene – ostensibly warranting expanding a BYOD policy so that it becomes a *WY*OD policy. *See* Robert D. Brownstone, *A "Wearables" Carol – Beware The Three Ghosts*, Digital Mountain E-Newsletter (May 27, 2015) <digitalmountain.com/enews/SPRING_2015_Article3.pdf> (citing a number of other Wearables articles); Nicole Black, *Wearables Are Here: Is Your Law Firm Ready?* Legal IT Professionals (Sep. 17, 2014) <http://www.legalitprofessionals.com/legal-it-

---

[141] *See* notes 65-66 above. *See also Successful eDiscovery in a Bring-Your-Own-Device Environment*, IT@Intel White Paper (June 21, 2012) <www.intel.com/content/www/us/en/it-management/intel-it-best-practices/ediscovery-with-byod.html>.

[142] *See, e.g.,* Good Technology, *Mobile App Containerization* (Nov. 11, 2014) <https://www1.good.com/secure-mobility-solution/mobile-application-containerization>; WeComply, *10 Tips for Creating a Successful BYOD Policy*, Today's General Counsel (July 8, 2014) <http://www.todaysgeneralcounsel.com/10-tips-creating-successful-byod-policy>; Ken Lienemann, *Containerization: Balancing BYOD for the Enterprise and You*, Innovation Insights (June 24, 2014) <http://insights.wired.com/profiles/blogs/containerization-balancing-byod-for-the-enterprise-and-you>; Janette Levey Frisch, *How Telecommuters Drive Home the Need for Confidentiality and Privacy Policies*, The Employerologist (June 12, 2014) <http://theemplawyerologist.com/2014/06/12/how-telecommuters-drive-home-the-need-for-confidentiality-and-privacy-policies/comment-page-1/>; RSA Security Agenda, *Securing the Next Wave of BYOD; Intel CISO Assesses Risks, Opportunities"* (Mar. 2013), available at .pdf p. 28) at <http://tinyurl.com/BYOD-Interview>; Penny Crosman, *Banks to Workers: 'Bring-Your-Own-Device' Party Is Over*, American Banker (Dec, 27, 2012) <http://www.americanbanker.com/issues/177_248/is-byod-going-away-1055466-1.html>; *Best Practices for Enabling Employee-owned Smart Phones in the Enterprise*, IT@Intel White Paper (Feb. 22, 2012) <http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/enabling-employee-owned-smart-phones-in-the-enterprise.html>.

columns/nicole-black/7000-wearables-are-here-is-your-law-firm-ready>; Green, *WYOD - is your organisation prepared for the wearable onslaught?* Info. Age (July 25, 2014) (focusing on the public sector in the UK) <www.information-age.com/technology/security/123458285/wyod-your-organisation-prepared-wearable-onslaught>.

3. NLRB Pronouncements as to Prohibitions/Restrictions on Blogging, Posting, Social-Networking and Tweeting

Determining an organization's official position on employee web postings is a much harder task than it appears at first glance. The spectrum of positions ranges from (1) actively encouraging employees to create and maintain content by providing them with the tools necessary to do so to (2) providing guidance about proper posting of content to (3) flat out prohibiting such postings (that approach could be illegal in certain circumstances). To determine where your (client's) organization falls on this spectrum requires a risk/benefit analysis. Consider not only the legal implications, but also the practical impact web activity and the organization's "web philosophy" can have.

When implementing written policies that address employees' work-related speech on social networking and other online sites, employers should consider requiring that employees observe appropriate guidelines when referring to the company, its employees, services and customers. The particular wording of `employers' social media policies is important.

Thus, each private sector employer – **whether or not its workforce is unionized**[143] -- should take the time to draft social media policies that will withstand NLRB scrutiny.[144] Over the past few years, the NLRB has increasingly targeted employers' social media restrictions – and adverse employment actions taken thereunder – as potential infringement on concerted activity rights under Section 7 of the NLRA. A strict position has been staked out in various NLRB promulgations:

- the March 31, 2015 NLRB social-media/profanity decision discussed at the end of this sub-section;
- this wide-ranging memo: NLRB, *Report of the General Counsel Concerning Employer Rules*, Memo No. GC 15-04 (Mar. 18, 2015) <http://apps.nlrb.gov/link/document.aspx/09031d4581b37135>;

[143] Karen McAndrew, *The NLRB and social media — why you need to care*, Vt. Emp. L. Letter (Apr. 13, 2014) <http://www.hrhero.com/techforhr/2014/04/the-nlrb-and-social-media-%E2%80%94-why-you-need-to-care/>.

[144] For drafting tips, *see* the ones cited and discussed in note 105 and accompanying text supra.

- at least nine other decisions by the Board in D.C., including at least two in 2014:[145]
    - one as to the Facebook "like" button,[146] as discussed in two articles by the author's colleagues;[147] and
    - another as to egregious conduct vitiating the protection of the Act;[148].
- a number of decisions by regional ALJ's, including *Kroger Co. of Michigan and Granger*, 199 L.R.R.M. (BNA) 1319 (ALJ Region 07 Apr. 22, 2014) <http://op.bna.com/elru.nsf/id/lbrd-9tpjzh/$File/KrogerCo.pdf>, now on appeal to Board as Case No. 07-CA-098566 <http://www.nlrb.gov/case/07-CA-098566>; *Boch Imports, Inc. d/b/a Boch Honda*, No. 1-CA-83551 (ALJ N.Y. Jan. 13, 2014) <http://op.bna.com/pl.nsf/id/kjon-9fslfj/$File/Boch%20Imports%20Inc..pdf>;
- settlement agreements with NLRB Regional Directors; and
- several lengthy reports promulgated by the NLRB's Acting General Counsel Lafe E. Solomon

The NLRB settlements and proceedings to date are non-conclusive as to where the pertinent boundaries may ultimately be drawn. Unfortunately, the NLRB's Reports – some containing internally inconsistent content – have created more confusion than clarity. Particular troubling are the NLRB GC's January 2012 Report's expressed displeasure with: "savings clauses" (that attempt to carve out protected discussions as to employment "terms and conditions"); and prohibitions on an employee's defamation (*i.e.*, untruthful disparagement) of the employer.

Equally befuddling is that Report's suggestion that a compliant social-media policy contain multiple examples of contexts in which individual's posts or tweets

---

[145] The other seven decisions are discussed in detail in the predecessor version of this White Paper: *Weyerhaeuser Co. and Ass'n of Western Pulp and Paper Workers*, 359 NLRB No. 138 (June 20, 2013) <mynlrb.nlrb.gov/link/document.aspx/09031d45812e8939>; *Hispanics United of Buffalo, Inc.*, 359 NLRB No. 37 (Dec. 14, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580e8c5f4>; *Bettie Page Clothing*, 359 N.L.R.B. No. 96 (Apr.19, 2013) <mynlrb.nlrb.gov/link/document.aspx/09031d458114449e>; *Dish Networks*, 359 NLRB No. 32 (Dec. 13, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580e85dc6>; *Karl Knauz Motors, Inc. W*, 358 NLRB No. 164 (Sep. 28, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580ccba21>; *In re DirectTV*, 359 NLRB No. 54 (Jan. 25, 2013) <mynlrb.nlrb.gov/link/document.aspx/09031d4580f1cab9>; *EchoStar Technologies*, 27-CA-066726, NLRB (Sept. 25, 2012) **(unpublished)** <mynlrb.nlrb.gov/link/document.aspx/09031d4580c8fc04>. *Costco Wholesale Corp.,* 358 NLRB No. 106 (Sep. 7, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580c45356>.

[146] *Three D, LLC d/b/a Triple Play Sports Bar and Grille*, 361 NLRB No. 31, Cases 34–CA 012915 and 34–CA–012926 (Aug. 22, 2014) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4581862ac8>.

[147] Dan McCoy and Sheeva Ghassemi-Vanni, Penalizing Employee Posts May Violate Protected Activity, Law360 (Oct. 14, 2014) <www.law360.com/employment/articles/582735?nl_pk=d89a7515-0be9-4a9b-a6eb-c1759d770289 >; McCoy and Ghassemi-Vanni, *NLRB Weighs in on "Like" Button*, F&W Emp. Brief (Sep. 17, 2014) <http://www.fenwick.com/publications/Pages/Fenwick-Employment-Brief---September-2014.aspx?WT.mc_id=EB_091714>.

[148] *Richmond Dist. Neighborhood Ctr.*, 361 NLRB No. 74, 20-CA-091748 (Oct. 28, 2014) (re-up for employment rescinded due to two employees' posts evincing egregious conduct and insubordination) <mynlrb.nlrb.gov/link/document.aspx/09031d458194a215>.

would run afoul of the given policy. Under the principle of *expressio unius est exclusio alterius* ("the express mention of one thing excludes all others"), a policy drafter would be hard pressed to craft a list of scenarios that does not implicitly authorize some types of inapt employee conduct.

Moreover, in April 2014, though not in a social-media or technology-acceptable-use case, the NLRB expressed concern about a behavior-standards policy provisions that "prohibit[ed] 'negative comments' and 'negativity [or gossip].'"[149] The Board found those dictates violative of the NLRA. Shortly thereafter, two of the author's colleagues aptly warned that "[e]mployers should keep the NLRB's penchant to heavily scrutinize seemingly neutral workplace policies firmly in mind, and take steps to ensure that their workplace policies do not overreach, no matter how benevolent the purpose."[150]

The NLRB's vigorous activity in the Web 2.0 arena was a harbinger of similar impingements on the right of an employer to govern employee use of the company-provided email system. In late 2014, the Board in D.C. held that employees previously granted access to the company email system must be allowed to use it to engage in protected communications on "nonworking time." *Purple Communications, Inc. and Communications Workers of America, AFL-CIO*, 361 NLRB No. 126 (Dec. 11, 2014) <http://www.nlrb.gov/case/21-CA-095151>. *See generally* Daniel J. McCoy and Sheeva J. Ghassemi-Vanni, Fenwick & West Emp. Brief (Jan. 2015) <fenwick.com/publications/Pages/Fenwick-Employment-Brief-January-2015.aspx>; Hogan Lovells, NLRB's decision in Purple Communications means employers must take a close look at policies restricting employee email use, Emp. Alert (Dec. 15, 2014) <ehoganlovells.com/cv/26dff83d1b1d15a7a289f26aa3848e5c5c6f82dd>; Jon Neidtiz, *Did Your Company's Email Policy Just Become Invalid?* Big Data Tech Law (Dec. 13, 2014) <datalaw.net/did-your-companys-email-policy-just-become-invalid/>.

The *Purple Communications* decision:

- overruled the Board's 2007 *Register Guard* decision discussed in detail in eWorkplace II, supra note 2 at 26, 33-35 (.pdf pp. 31, 38-40) <http://www.fenwick.com/Fenwickdocuments/Eworkplace_Privacy_Social-Media_Materials_Neli_Brownstone_4-3-12.pdf>; and

- even went farther than the D.C. Circuit decision that had reversed the Board's 2007 *Register-Guard* decision, also discussed at *id.*

The practical ramifications of *Purple Communications* are not yet clear. The ostensibly pro-employer exceptions in that opinion – including the unrealistic focus on "nonworking time" -- seem quite hollow. However, it is possible that a "savings clause" and other careful drafting can still enable an "incidental" or "limited" personal-use exception to pass muster even under the new NLRB approach.

---

[149] *Hills and Dales Gen'l Hosp.*, 360 NLRB No. 70 (Apr. 1, 2014) <http://mynlrb.nlrb.gov/link/document.aspx/09031d45816688cc>.

[150] Daniel J. McCoy and Dan Ko Obuhanych, *NLRB Continues to Scrutinize Employee Handbook Provisions*, Fenwick Emp. Brief (Apr. 21, 2014) <http://www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-April-2014.aspx?WT.mc_id=EB_042114>.

Following *Purple*, in 2015 the NLRB issued yet another pro-employee social-media decision. The Board found that the below Facebook post constituted "protected, concerted comments" under the NLRA: "Bob is such a NASTY MOTHER FUCKER don't know how to talk to people!!!!!!! Fuck his mother and his entire fucking family!!!! What a LOSER!!!! Vote YES for the UNION!!!!!!!" *Pier Sixty, LLC*, 02-CA-068612 (Mar. 31, 2015) <http://www.nlrb.gov/case/02-CA-068612>. In addition, the NLRB found that because the employer "tolerated the widespread use of profanity in the workplace, including the words 'fuck' and 'motherfucker' [such that] his Facebook post would not cause him to lose the protection of the Act." *Id.* Thus, it upheld the ALJ's ruling that the post was not an apt basis on which to discharge the employee. *See also* Daniel J. McCoy and Sheeva Ghassemi-Vanni, *Terminating Employee for Calling Boss a "Nasty Mother F**ker" Violated NLRA*, Fenwick Emp. Brief (Apr. 24 2015) </www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-April-2015.aspx>.

In sum, until there is a pertinent appellate decision, legal standards are still not settled as to which prohibitions would and would not constitute unfair labor practices.

C. Risks of Strict Policies

1. Creation of Duty to Act?

An employer's *right* to monitor is distinct from a *duty* to monitor. If an employer actually monitors (instead of just having employees acknowledge in writing that the employer reserves the right to do so), it should allocate resources to follow through and review the electronic activity and properly address any inappropriate conduct. For example, at the least in the harassment context, failure to do so may result in potential vicarious liability to third parties – based on actual or constructive knowledge of harmful activities plus the failure to remedy.

2. Don't Prohibit All Innocent Surfing

An employer, however, should be cautious of having overbroad web-surfing restrictions, especially if it only plans to enforce such limits selectively.[151] One viable option is to craft a realistic policy that acknowledges employees may engage in incidental personal use of the Internet as long as such use does not interfere with the employee's duties. Going the overly strict route in the written document but then hardly ever enforcing leaves can leave an organization open to charges of arbitrary and discriminatory conduct.[152] When policies treat disparate groups of employees differently, inconsistent enforcement of the established categories can lead to troublesome disputes. A highly publicized example occurred last year at Harvard University. There an email policy went awry when the administration decided to apply an approach that deemed certain faculty members "staff" rather than "faculty." Bill Donahue, *How To Keep An Eye On Workers But Keep Out Of Trouble*, law360 (Mar. 18, 2013) <morganlewis.com/pubs/Law360_KeepAnEyeOnWorkers_18march13.pdf>

[151] *Compare* the NLRA issue discussed in **Section II(B)(4)** above.

[152] *See, e.g., Dep't Of Education v. Choudhri*, OATH Index No. 722/06 (N.Y.C. Office Of Admin. T & H Mar. 9, 2006) <http://files.findlaw.com/news.findlaw.com/hdocs/docs/nyc/doechoudri30906opn.pdf>.

D. Periodic Training

Some identify the fundamental principles of implementation as "The Three E's" of Establish, Educate and Enforce.[153] Having **Established** written policies, employers should not only provide **Education** on policies' contents but also strive to **Enforce** as consistently as possible.[154] Nowadays, many creative ways to train are available, including interactive modules and policy portals[155] – and short videos such as the three ones linked in Section V(E) below..

E. Information-Security Compliance Considerations[156]

In general, HR should collaborate with IT on information-security issues.[157] For pertinent resources, *see* the author's extensive Bibliography,[158] which, among other items, links to this short video: Robert D. Brownstone, *Top 3 Concerns in Data Security,* Fenwick & West LLP (Nov. 2012) <http://fenwick.com/Videos/Pages/Top-3-Concerns-in-Data-Security.aspx>.

Two best practices warrant mentioning here:

- **Encryption** of data in transit and at rest should be a high priority, especially on laptops– and as to highly sensitive information wherever stored.[159]

---

[153] *See* Nancy Flynn, *The e-Policy HANDBOOK*, at Ch. 20 ("Employee Education Policies and Best Practices"), at 173 (2d ed. 2009) <tinyurl.com/3-Es-Flynn>.

[154] Lothar Determann and Ute Krudewagen, *Policing Social Media*, Recorder (Apr. 6, 2012) <http://tinyurl.com/Policing-Social-Media>; Cori Stirling, *Regulating Employee Personal Conduct Through Employment Policies; Careful Wording and Consistent Enforcement of Non-Fraternization and Social Media Polices are Key to Avoiding Legal Liability*, Dinsmore (Mar. 16, 2012) <dinsmore.com/regulating_employee_personal_conduct>.

[155] Michael Rassmussen, *Policy Communication in a YouTube World*, Compliance Week (Sep. 25, 2012) <www.complianceweek.com/news/news-article/policy-communication-in-a-youtube-world>.

[156] The SEC has focused increased attention on publicly traded companies' cybersecurity and data breach prevention. *See, e.g.*, SEC Division of Corporation Finance ("CF"), *CF Disclosure Guidance: Topic No. 2; Cybersecurity* (Oct. 13, 2011) <sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>. Moreover, those representing or working for broker-dealers will want to look at the SEC's Office of Compliance Inspections and Examinations' ("OCIE's") National Exam Program Risk Alerts <sec.gov/ocie> (last visited July 4, 2014), especially this one: OCIE CYBERSECURITY INITIATIVE (Apr, 15, 2014) <www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf>.

[157] Daniel Schwartz, *Data Privacy and Human Resources: A Target to Aim For?* Connecticut Emp. L. Blog (May 6, 2014) <ctemploymentlawblog.com/2014/05/articles/data-privacy-and-human-resources-a-target-to-aim-for/>.

[158] <http://www.fenwick.com/professionals/Pages/bobbrownstone_insights.aspx>.

[159] Robert D, Brownstone, *Safeguards against Data Security Breaches (Part One)*, Fenwick & West LLP (Mar. 2013) (very short video regarding encryption) <http://fenwick.com/Videos/Pages/Safeguards-against-Data-Security-Breaches-Part-one.aspx>.

- **Role-based-access-control ("RBAC")** should be used to limit the number of people who even get to see certain vats of information, let alone download, carry around or transmit such information.[160]

RBAC is especially important as to personnel "files," [161] which could be stored on shared network drives, in databases and/or off-site with a service provider (*i.e.*, in "The Cloud").

A stark reminder of the need for those very measures, including as to data regarding an organization's own employees, is the 2014 situation in which a "U.S. Internal Revenue Service employee took home a computer thumb drive containing unencrypted data on 20,000 fellow workers." Richard Rubin, *IRS Employee Took Home Data on 20,000 Workers at Agency*, Bloomberg (Mar. 18, 2014) (noting that the IRS claimed "[t]he information dates to 2007, before the IRS started using automatic encryption") <http://www.bloomberg.com/news/2014-03-18/irs-employee-took-home-data-on-20-000-workers-at-agency.html>.

[160] Robert D, Brownstone, *Safeguards against Data Security Breaches (Part Two)*, Fenwick & West LLP (Ap. 2013) (very short video regarding RBAC) <http://fenwick.com/Videos/Pages/Safeguards-against-Data-Security-Breaches-Part-Two.aspx>.

[161] For an overview of the three RBAC aspects of a modern day "personnel file," *see* Robert D. Brownstone, *Electronic Records Retention – Preserve or Perish; Destroy or Drown*, at 8-10, Nat'l Const. Conferences (Mar. 20, 2014) <http://www.itlawtoday.com/files/2014/05/NCC_Retention_3-20-14_%C2%A9_FWLLP_RBrownstone.pdf>.

Appendix A – Brownstone Bibliographies (8/2/15)

1. Acceptable-Use & Social-Media Policies – Links to Many SAMPLES*
   - <http://tinyurl.com/SampleTAUPSLatestFWLPP>

2. eDiscovery – General/Overall*
   - <http://tinyurl.com/eDiscoBiblioLatestFWLPP>

3. eDiscovery – Social Media*
   - <http://tinyurl.com/SocialMediaeDiscoLatestFWLPP>

4. Employees' Attorney-Client Privilege vs. eWorkplace Policies*
   - <http://tinyurl.com/ACPvTAUPBiblioLatestFWLPP>

5. Ethics in Litigation re: Social-Media for Lawyers, Jurors & Judges*
   - <http://tinyurl.com/SocialMediaEthicsLatestFWLPP>

6. ITLawToday – Bob's Blog
   - Home: <http://www.ITLawToday.com>
   - Resources: <http://www.itlawtoday.com/resources/>

7. Whole Brownstone Bibliography *(including articles, slide decks & press coverage)*
   - <fenwick.com/bobbrownstoneinsights>

***** *To get the full functionality of any of these .pdf files, download a copy.*

NELI PSEEO

APP. B

(as revised 8/20/15)

August 2015

San Francisco

The eWorkplace – Protecting Employer Information v. Employee Privacy

THESE MATERIALS ARE MEANT TO ASSIST IN A GENERAL UNDERSTANDING OF CURRENT LAW AND PRACTICES.

THEY ARE NOT TO BE REGARDED AS LEGAL ADVICE.

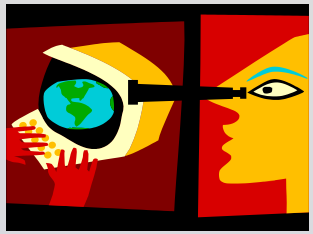
THOSE WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

Robert D. Brownstone, Esq.

Outline/ Agenda

- I. INTRO – THE MODERN LANDSCAPE
- II. "MONITORING"
- III. INVESTIGATIONS
- IV. SEARCHING AND TRACKING
- V. IMPLEMENTING COMPLIANCE POLICIES *(quick overview)*

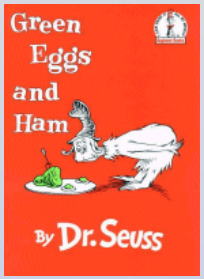
I. INTRO – A. Our Digital World



- **Modern differences:**
  - **"Frolic & detour" track-able (but best to disclose tracking)**
  - **Internet of Things (IoT)**
    - **Thingful and Shodan search engines**
    - **Wearables**

I. B. Strange Things People Memorialize

- "Multiple Audiences" Test
- "Green Eggs & Ham" Test:
  - Would you like it in the press?
  - Would you like it on a competitor's desk?
  - Would you like it in the government's hand?
  - Would you like to read it on the witness stand
- If the content will get you slammed, then....



DO NOT SEND OR POST IT, SAM I AM

- Even if use Gmail, don't rely on "Undo Send"

I(B). Strange Things *(c't'd)* – 1. Liability Evidence

- **Sony Emails re:, *e.g.*, Pres. Obama:**

Date	2013-11-26 16:25:50 UTC
From	sr@scottrudinproductions.com
To	amy_pascal@spe.sony.com

On Nov 26, 2013, at 8:20 AM, "Scott Rudin" <sr@scottrudinproductions.com> wrote:

Re: 12 YEARS.

On 11/26/13 11:05 AM, "Amy Pascal" <Amy_Pascal@spe.sony.com> wrote:

I doubt it
Should I ask him if he liked DJANGO

On Nov 26, 2013, at 8:01 AM, "Scott Rudin" <sr@scottrudinproductions.com> wrote:

Re: Would he like to finance some movies?

On 11/26/13 9:55 AM, "Amy Pascal" <Amy_Pascal@spe.sony.com> wrote:

What should I ask the president
At this stupid Jeffrey breakfast
A

I(B)(1). Strange Things *(c't'd)*

- **Even judges & lawyers:**

From: "Chief Judge Rader, Randall R." <RR@cafc.uscourts.gov>
Date: March 5, 2014 at 3:24:12 PM EST
To: Edward Reines <edward.reines@weil.com>
Subject: Congratulations

Ed,

On Wednesday, as you know, the judges meet for a strictly social lunch. We usually discuss politics and pay raises. . . . .

You were alone and IMPRESSIVE in every way. In both cases, you knew the record cold and handled every question with confidence and grace. She said that she was really impressed with your performance. Two of my other colleagues immediately echoed her enthusiasm over your performance.

In sum, I was really proud to be your friend today! You bring great credit on yourself and all associated with you!

And actually I not only do not mind, but encourage you to let others see this message.

Your friend for life, rrr

- *In re Reines*, **771 F.3d 1326 (Fed. Cir. 11/5/14)**

- **And even the TSA . . .**

- **Carly Ledbetter, *TSA Spokes-person Tweets Photo Of '$75,000' In Luggage, Internet Gets Angry*, Huffington Post (7/1/15)**

I(B)(1). Strange Things *(c't'd)*

- **Deflategate texts, *e.g.*:**

Date and Time	Sender	Recipient	Message
01/19/2015 07:25:18 EST	John Jastremski (508) 958-xxxx	Tom Brady2[63] (917) 704-xxxx	Call me when you get a second

Date and Time	Sender	Recipient	Message
01/19/2015 09:51:54 EST	Tom Brady2 (917) 704-xxxx	John Jastremski (508) 958-xxxx	You good Jonny boy?
01/19/2015 09:53:27 EST	John Jastremski (508) 958-xxxx	Tom Brady2 (917) 704-xxxx	Still nervous; so far so good though. I'll be alright

- **March Wells report, at pp. 102-04 (.pdf pp. 106-08)**
- ***See also* July ruling, at pp. 4 & 11-13**

I(B). 2. Internet – Social-Media

- **Now, with Web 2.0/UGC, a bigger universe of web activities [many via Fenwick & West clients ☺]**
- **Focus here on risks, not rewards**
- **Social-Media Policy – or Technology Acceptable Use Policy ("TAUP") provision – to address:**
  - **1) General Guidelines**
  - **2) Employer-Sponsored**
  - **3) Personal**

I(B)(2). Social- Media Policies – esp. in Public Sector

- **NASCIO, *Examining State Social Media Policies: Closing the Gaps* (6/6/13), including 2 Checklists and:**
  - **Sample Social Media Policy (Mass.) re:**
    - ***Required Work-Related Use of Social Media* – Guidelines for contributors and moderators, including:**
      - **Considerations When Speaking on Behalf of your Agency**
      - **Understand Users' First Amendment Rights**
      - **Protect Confidential Information**
      - **Respect Your Audience & Your Coworker**

I(B)(2). Sample Social Media Policy *(c't'd)*

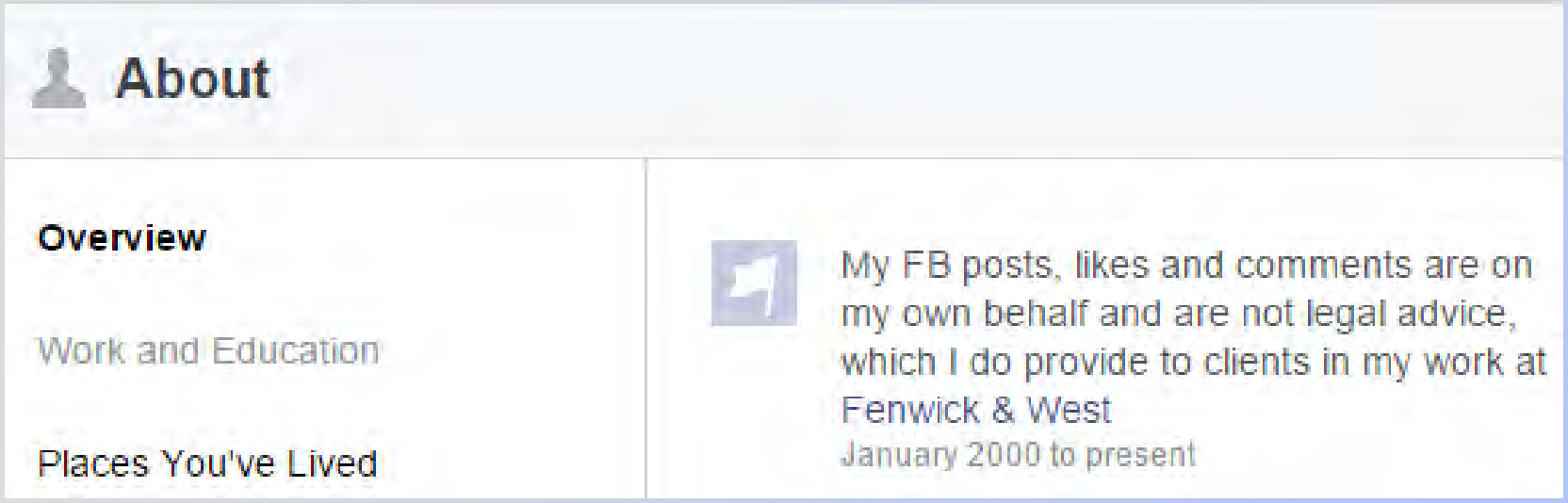
- ***Personal Use of Social Media at Work***
  - **a. Follow the Acceptable Use Policy**
  - **b. Employees' personal use should not be attributable to the agency or to the employee's job function at agency**
  - **c. Must be in conformance with relevant portions of workplace policies [Codes of Conduct and / or TAUP?] and all relevant laws and regulations**
  - **d. Must not be excessive**
- ***Personal Use of Social Media outside of Work***
  - **a. Employees' personal use should not be attributable . . .**
  - **b. Must be in conformance with . . .**

I(B)(2). Internet – Social-Media *(c't'd)*

- **Drafting & Enforcement Tips?**
  - **Industry-specific? (FDA – Paper at 11)**
  - ***See* sample language in Paper at 31 re:**
    - **1) no lying**
    - **2) no disclosure of confidential proprietary information or intellectual property unless:**
      - **authorized; or**
      - **essential re: concerted action re: terms/conditions of employment**
        - **COMPARE NLRB Memo No. GC 15-04**
    - **3) disclaiming speaking authority . . .**

I(B)(2). Internet – Social-Media *(c't'd)*

- **Disclaimers (incl. for Lawyers)** *(c't'd)*
  - **Facebook trickier than others**
    - **Under "Work", I input into first "Position" field some language ending with " . . . at"**



I(B)(2). Internet – Social-Media *(c't'd)*

- **Facebook non-lawyer disclaimer**

My Facebook posts, likes and comments are on my own behalf and not on behalf of my employer or part of my work at [COMPANY NAME]

I(B)(2). Internet – Social-Media *(c't'd)*

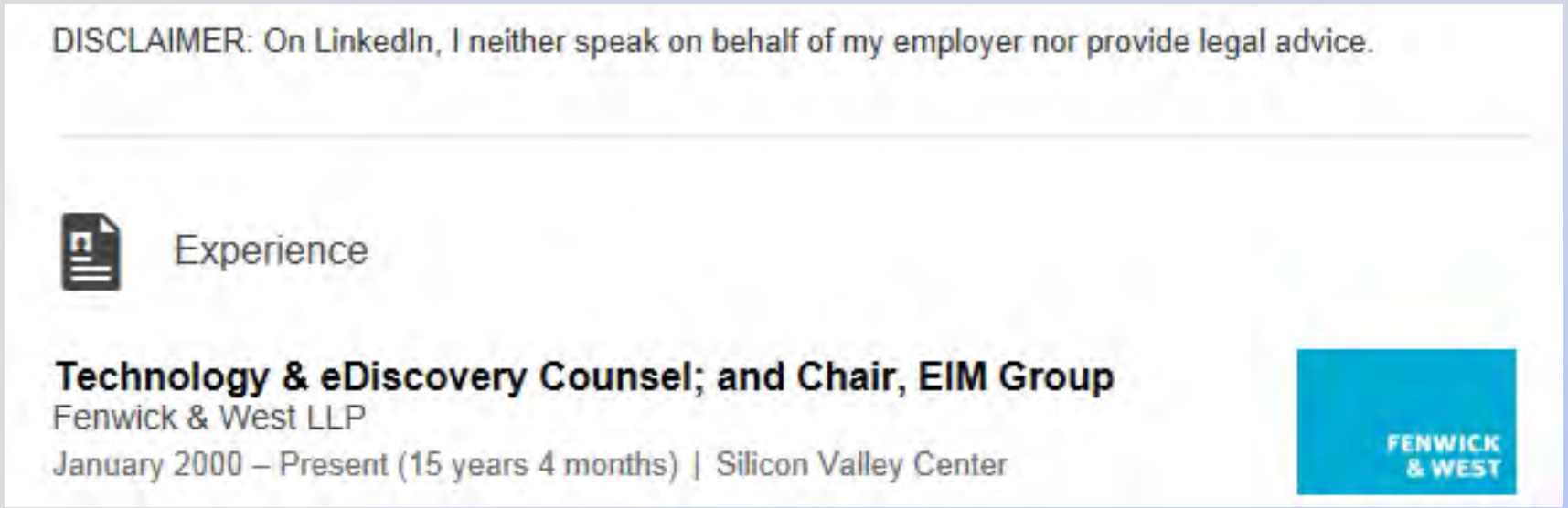
- **Disclaimers (incl. for Lawyers)** ***(c't'd)***
  - **Twitter (Profile . . . Edit)**

I(B)(2). Internet – Social-Media *(c't'd)*

- **Twitter non-lawyer disclaimer**

I(B)(2). Internet – Social-Media *(c't'd)*

- **LinkedIn lawyer disclaimer**



I(B)(2). Internet – Social-Media *(c't'd)*

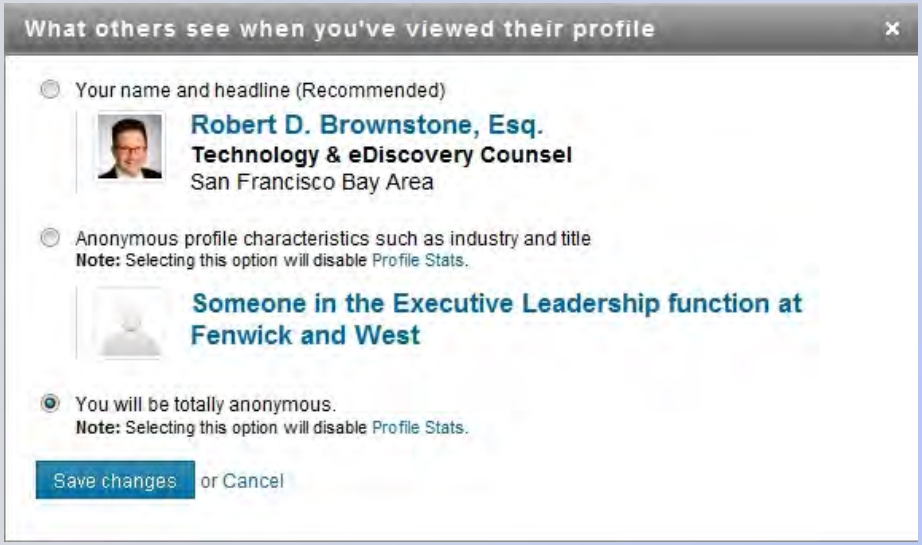
- **LinkedIn non-lawyer disclaimer**

DISCLAIMER: On LinkedIn, I speak on my own behalf and not on behalf of my employer.

Experience

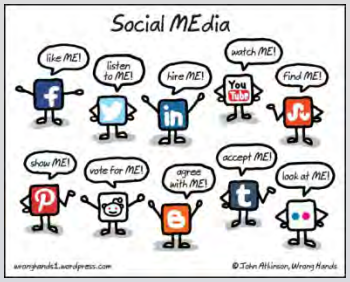
I(B)(2). Internet – Social-Media *(c't'd)*

- **Unique LinkedIn issues**
  - **Recommendations? Endorsements?**
  - **Transparent profile searching?**



  - ***See also* NYCLA, *The ethical implications of attorney profiles on LinkedIn*, Prof'l Ethics Comm. Formal Op. 748 (3/10/15)**

I(B)(2). Social-Media eDiscovery



- **Now a big body of case-law:**
  - Social-Media eDiscovery Biblio
  - General eDiscovery Biblio
  - Social-Media Ethics Bibliography
- **Some '14 Harassment/"Rummaging" Exs:**
  - *Ogden v. All-State Career School*, 299 F.R.D. 446 (W.D. Pa. 4/23/14)
  - *Doe v. Rutherford Cty. Bd. Of Ed.*, 2014 WL 4080159 (M.D. Tenn. 8/18/14) (some deletion)
- **Posts' Search-ability:**
  - **NEW!** Sarah Frier, *Twitter Reaches Deal to Show Tweets in Google Search Results*, Bloomberg (2/4/15)

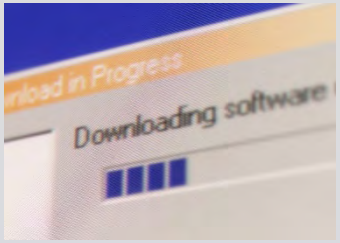
I(B)(2). Social-Media eDiscovery *(c't'd)*

- **Posts' Capture-ability (many ways):**
  - **Some low tech, e.g.:**
    - **Paper print out***
    - **Screen capture***
    - **Adobe Acrobat PDFMaker icon in IE**
  - **Some high tech, e.g.:**
    - **X1 Social Discovery *(presenter has used)***
    - **PageFreezer (incl. WebPreserver.com)**
    - **Page Vault**
    - **Smarsh Social Media Archiving**

***- Authentication concerns ?? . . .**

- **Results may vary**
- ***See* decisions in articles at p. 1 of above Biblio**

I(B)(2). Social-Media eDiscovery *(c't'd)*



- **Authentication?** ***But see:***
  - ***Jaszczyszyn*** **and** ***Ehling*** **decisions at Paper pp. at 20, 22 & 40**
  - **Various exs. throughout August '11 & January '12 NLRB GC Reports linked in materials**
- **Not Reasonably Accessible?**
  - **Facebook**
    - ***"Download Your Information"***

      [instructions available on request]
  - **Twitter**
    - ***"Your Twitter Archive"***

I(B)(2). Social-Media eDiscovery *(c't'd)*

- **Judges more and more forceful:**
  - **offering to "friend" witness and do "in camera" review of posts and photos**
    - ***Barnes v. CUS Nashville, LLC*, *[d/b/a Coyote Ugly Saloon]*, 2010 WL 2265668 (M.D. Tenn. 6/3/10)**
  - **requiring party itself to disclose his/her FB login/password**
    - ***White Tail Oilfield Services*, 2012 WL 4857777 (E.D. La. 10/11/12) (FB's "Download Your Information")**

I(B)(2). Social-Media eDiscovery *(c't'd)*

- **Judges more forceful** *(c't'd)*
  - **compelling juror's consent to FB production**
    - ***Juror No. One v. Superior Court (Royster)*, 206 Cal. App. 4th 854, 142 Cal. Rptr. 3d 151, 153 (3 Dist. 5/31/12)**
  - ***Compare* this Gmail "consent" decision:**
    - ***Negro v. Super. Ct. (Navalimpianti)*, 230 Cal. App. 4th 879, 179 Cal. Rptr. 3d 215 (Cal. App. 6 Dist. 10/21/14) (consent volitional even though faced with choice between consenting or facing sanctions)**

I(B)(2). Social-Media eDiscovery *(c't'd)*

- **Preservation/Spoliation & Collection (incl. Lawyers' Ethical Duties)**
  - ***Account Deactivation*** **in ≥ 4 decisions, incl.**
    - ***Crowe v. Marquette Transp.*****, 2015 U.S. Dist. LEXIS 9198 (E.D. La. 1/20/15) (deactivation vs. permanent deletion)**
    - ***Chapman v. Hiland Operating*****, 2014 WL 2434775 (D. N.D. 5/29/14) (deactivation)**
  - ***"Clean up" if in LIT Hold mode***
    - ***Lester v. Allied Concrete*** **(Va. Cir. Ct. 9/1/11 & 10/21/11), linked from p. 5 of above Ethics Biblio**
    - **Fl. Bar. Prof. Ethics, *(Proposed) Advisory Op. 14-1* (1/23/15) (OK to remove if preserve a copy)**

I(B)(2). Social-Media eDisco & Lawyer Ethics *(c't'd)*

- **Preservation/Spoliation**
  - ***Deletions (texts too)*:**
    - *Painter v. Atwood*, 2014 WL 1089694 (D. Nev. 3/18/14)
  - ***Deflategate Adverse Inference*** **[both quoting me a lot ☺]:**
    - Rebekah Mintzer, *'Deflategate' Lessons for E-Discovery Device Policies*, Corp. Counsel (5/18/15)
    - **NEW!** Rebekah Mintzer, *Deflation to Spoliation? Tom Brady and E-Discovery*, Corp. Counsel (7/31/15)

I(B)(2). Social-Media eDisco & Lawyer Ethics *(c't'd)*

- **Preservation/Spoliation** *(c't'd)*
  - ***FRCP 37(e) to change 12/1/15***
    - this color-coded mark-up **of key changes, at slides 15-19**
    - clean version of rules set **as sent to Congress by U.S. Supreme Court (4/29/15), at pp. 24-26 (.pdf pp. 27-29)**
    - full report with Advisory Committee Notes **(5/1/14), at pp. 306-30, et seq.**
  - ***Public entities – FOIA / Self-Collection*:**
    - **Peter Scheer,** ***Hillary's email problem: A crucial lesson for government officials everywhere*****, FAC (3/17/15)**
    - **Jon Neiditz,** ***. . . Clinton Email & Information Governance Issues*** **. . . , Big Data Tech Law Blog (3/16/15)**
    - **Thomas Kaplan,** ***Cuomo's Rule on Purging State Email Roils Albany*****, NYT (3/12/15)**

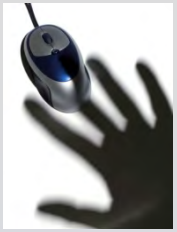
I(B)(2). Social-Media eDisco & Lawyer Ethics *(c't'd)*

- **Own Client's Postings day-to-day**
  - **No clean-ups; but OK to "private"-ize**
    - **Pa. Bar Ass'n, *Formal Op. 2014-300* (9/16/14)**
  - **No removal if would be spoliation**
    - **N.C. Bar, *Formal Ethics Op. No. 5* (7/25/14)**
  - **OK to delete IF not spoliation or illegal**
    - **Phila. Bar Ass'n, *Op. 2014-5* (7/7/14)**

I(B)(2). Social-Media eDisco & Ethical Duties *(c't'd)*

- **Jurors**
  - **Lots of rules and opinions regarding jurors and lawyers who research them**
    - ➢ ***See* above Ethics Biblio**
    - ➢ **Be careful with LinkedIn profile-surfing. Compare:**
      - ✓ **NYSBA Guidelines (3/18/14); NYCLA, *Op. No. 743* (5/18/11); and ABCNY, *Formal Op. 2012-2*; *JURY RESEARCH AND SOCIAL MEDIA* (6/4/12)**
      - ✓ **with ABA, *Formal Op. 466* (4/23/14)**
- **Judges**
  - **Lots of ethics ops. re: judges' SNS activities**
    - ➢ ***See* above Ethics Biblio**

II. Monitoring – Risk-Management Concerns



- **All of the above . . . plus . . .**
- **Protecting Individuals' PII**
  - **47+ "states" statutes re: notice-of-breach and other anti-identity-theft issues [KY in 2014]**
  - **≥ 22 of those state laws apply to public sector**
  - **Notice of breach statute triggered by residence state of affected person**
  - **Encryption**
    - **I recommend it be used broadly**
    - **Only required in MA (by OCABR regs)**

II. Monitoring – Justifications *(c't'd)*

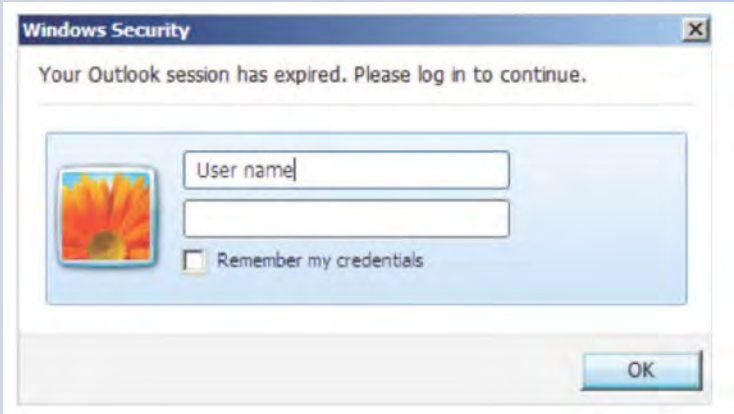
- **PII** *(c't'd)*
  - **FTC quite active in FTC Act enforcement**
    - **only re: private sector**
      - ***See* *Wyndham* and FTC (*LabMD*) decisions re: FTC enforcement authority (each on appeal to a Cir. Ct.)**
      - ***See also* Complaint, *Reitinger v. FTC* (D.D.C. 5/13/15)**
    - **no authority re: non-profits or state/local gov't**
      - ***But see* FTC Safeguards Rule under G-L-B as to Complaint filed with FTC by privacy advocate EPIC re: educational institution's 2013 data breach**
        - **Discussed here and there**
        - ***See also* this 9/29/14 PCWorld article**

II. Monitoring – Justifications *(c't'd)*

- **Protecting Individuals' PHI**
  - **HIPAA Final HHS Regs (9/23/13)**
    - **HHS active, under HIPAA, even as to public sector:**
      - **State (2012) – Alaska Dep't of Health & Social Servs.**
      - **Local (2014) – Skagit County, WA**
  - **7 states [AR, CA, MO, NV, ND, TX & CT (insurers)]**
  - **NEW! NJ S.B. 562 requiring health insurance carriers to encrypt PHI *and* PII (eff. 8/1/15)**

II. Monitoring – Justifications *(c't'd)*

- **Phishing Schemes and Malware**
  - **What is:**
    - **Phishing?**
    - **(Spear-) phishing?**
    - **Social Engineering?**
      - ***See, e.g.,* this article re: . . .**



II. Monitoring's Legality – Some Highlights

- **On whole, same rules (two keys) continue to apply re: viability of "reasonable expectation" element for invasion claim theories based on:**
  - **Constitution (federal and/or state)**
  - **Statutes (federal and/or state)**
  - **Common law (case law)**

II. Monitoring *(c't'd)* – First Amendment

- **Some decisions discussed at *eWorkplace III*, at 22-24 (.pdf pp. 27-29)**
- **Capacity as public employee or private citizen?**
  - **Many relatively recent police-officer decisions, *e.g.*, *Duke v. Hamil*, 2014 WL 414222 (N.D. Ga. 2/4/14) (Confederate flag Facebook posting; demotion; Univ. PD interest in non-disruption and efficiency trumped 1st A.)**
- **"Liking" a Facebook page = protected speech?**
  - ***Bland v. Roberts*, 730 F.3d 368 (4th Cir. 9/23/13) ("liking a political candidate's campaign page. . . . is substantive speech")**

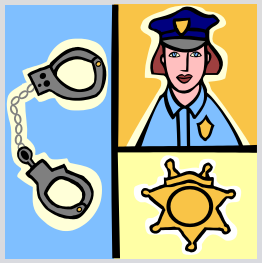
II. First Amendment *(c't'd)* – Some Other Decisions

- **Faculty speech related to scholarship or teaching:**
  - ***Demers v. Austin*, 2014 WL 306321, at *1 (9th Cir. 1/29/14)**
    - **Discussed, with other authorities, in FAC, *A&A: Prof worried about free-speech rights regarding Facebook post* (2/22/15)**
- **First appellate decision re: public-employee's blog posts and twitter tweets**
  - ***Naffe v. Frey*, 789 F.3d 1030 (9th Cir. 6/15/15)**
    - **Discussed in Amanda Bronstad, *Prosecutor Wins Appeal Over His Tweets Against Activist* , Nat'l L.J. (6/16/15)**

II. Monitoring *(c't'd)* – 4th Amendment

- **USSC 4th A. opinion's potential impacts:**
  - ***Riley v. Cal.*, 134 S. Ct. 2473 (2014)**
    - **No diminishment of employer's rights to its own devices or data stored on devices owned by employees**
    - **Public sector employees may now argue employers need to tread more carefully in investigatory searches**
      - ***Quon v. Arch Wireless*, 529 F. 3d 892 (9th Cir. 2009) – dueling opinions re: *O'Connor v. Ortega* (U.S. 1987)**
      - ***But see Liebeskind v. Rutgers Univ.*, 2014 WL 7662032, (N.J. App. 1/22/15) (unpublished opinion upholding state university's extraction of employee's internet browsing activity in light of broad, clear TAUP)**

II. Monitoring *(c't'd)* – 4th A *(c't'd)* –



- ***Riley*'s impacts** *(c't'd)*
  - **Local storage concerns if . . . seizure + warrant**
  - **Implicitly sends message to employers to be quite clear in policies (and training), including as to BYOD**
    - ***Ontario v. Quon*, 560 U.S. 46 (U.S. 6/17/10)**

II. Monitoring *(c't'd)* – BYOD [(post-*Riley* (seizure case)]

- **BYOD = bring your own device**
- **COPE = corporate-owned, personally enabled**
  - ***Creating a Successful BYOD Policy*, Symantec (2/14/13)**
- **WYOD ?!**
  - **Brownstone, *A "Wearables" Carol – Beware The Three Ghosts*, Digital Mountain E-Newsletter (Spring 2015)**
  - **Green, *WYOD - is your organisation prepared for the wearable onslaught?* Info. Age (7/25/14) (UK pub. sector)**

II. Monitoring *(c't'd)* – BYOD *(c't'd)*

- **As to iCloud sync, *see* this SCA case:**

  Sunbelt Rentals v. Victor, 2014 WL 4274313 (N.D. Cal. 8/28/14)

- ***Compare* Rajaee v. Design Tech Homes, 2014 WL 5878477 (S.D. Tex. 11/11/14) (remote-wipe OK)**

II. Monitoring *(c't'd)* – BYOD/COPE *(c't'd)* –

- **eDiscovery: "possession/ custody/ control" issue re: workers' own devices, webmail or texts**
  - ***Small v. Univ. Med. Ctr. of S. Nev.*, 2014 WL 4079507 (D. Nev. 8/18/14), as discussed *here***
  - ***Puerto Rico Telephone v. San Juan Cable*, 2013 WL 5533711 D. P.R. 10/7/13) (YES where presumably knew 3 officers used personal email accounts to manage company business)**
  - ***Cotton v. Costco Wholesale Corp.*, 2013 WL 3819974 (D. Kan. 7/24/13) (NO as to texts sent from personal phones; harassment/discrimination case)**
- **Deflategate – what if it were a lawsuit?**

II. BYOD/ COPE *(c't'd)* –

- **Hilary Clinton situation**
  - **Ed Silverstein, *Officials Reveal Clinton Sent Classified Info Through Her Private Server*, Legaltech News (7/24/15)**
- **Pending Cal. Sup. Ct. case**
  - **"Are written communications pertaining to city business, including email and text messages, which (a) are sent or received by public officials and employees on their private electronic devices using their private accounts, (b) are not stored on city servers, and (c) are not directly accessible by the city, 'public records' within the meaning of the California Public Records Act?"**
    - ***San Jose v. Superior Court* (*Smith*), 169 Cal. Rptr. 3d 840 (Cal. App. 6 Dist. 3/27/14) *depublished on grant of review*, 326 P.3d 976 (6/25/14)**
    - ***California Supreme Court takes up issue of government e-mails on personal smartphone*, First Amend. Coalition (7/10/14)**

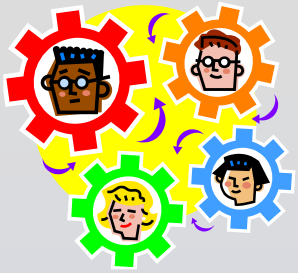
II. Monitoring *(c't'd)* – Privacy Expectations *(c't'd)*

- ***Aside from SOME 1st and 4th A. claims*, typically courts support employer . . . . BUT . . .**
- **Two potential exceptions:**
  - **examining locally-stored files impinging on employee's attorney-client (a/c) privilege**
    - ***See* this ACP-vs.-TAUP Bibliography**
  - **illicitly obtainment of log-in credentials and unauthorized access of content in personal account**
    - ***See* Paper at 20-22**
    - ***See also* *Brautigam v. East Whittier Sch. Dist.*, Minute Order, No. BC541803 (Super. Ct. L.A. 1/5/15)**
      - **Marisa Kendall, *Blurring of Work, Personal Tech Drives Privacy Disputes*, Recorder (1/30/15) [quoting me ☺]**
      - **$275K Settlement (3/26/15)**

II. Another Issue – Concerted Action

- **NLRB Social-Media Promulgations**
  - **≥ 10 NLRB decisions since Sep. '12**
  - ***GC Reports*, complaints, settlements & ALJ decisions (INCLUDING 3/8/15 Report and 5/30/12 Report)**
  - **Circuit court decision some day**
- **NLRB Email Usage Decision**
  - ***Purple Communics.*, 361 NLRB No. 126 (12/11/14)**
    - **"nonworking time" rule unworkable IMHO**
- ***See* Paper at 31 & 45-48**

II. Concerted Action *(c't'd)*



- **Recent NLRB Decisions**
  - **"Like" Button, etc.**
    - ***Three D, LLC d/b/a Triple Play Sports Bar and Grille*, 361 NLRB No. 31, Cases 34–CA 012915 and 34–CA–012926 (8/22/14) (now on appeal to Second Circuit)**
  - **Concerted but Egregious so not Protected**
    - ***Richmond Dist. Neighborhood Ctr.*, 361 NLRB No. 74, 20-CA-091748 (10/28/14) (re-up for employment rescinded), as discussed *here***
  - ***Terminating Employee for Calling Boss a "Nasty Mother F**ker" Violated NLRA***
    - ***Pier Sixty, LLC*, 02-CA-068612 (3/31/15) (also going to 2d Cir.)**

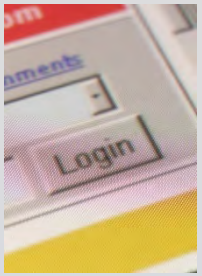
III. Investigations and Background Checks

- ***Criminal history ["Ban the Box"]***
  - **≈ 20 states (incl. MA) stricter than EEOC**
  - **NEW! NYC "Fair Chance Act" Ordinance: amending Admin. Code § 8-107(10)-(11) (eff. 9/27/15)**
    - **Summary: "New York City Passes Ban-the-Box Ordinance"**
- ***Credit report information***
  - **EEOC & FTC, *Background Checks: What Employers Need to Know* (3/10/14)**
  - **≥ 11 states' laws (incl. DE as to public employers); and NYC too (as of 9/2/15). NJ bill pending.**

III. Investigations and Background Checks

- ***General Web Surfing re: Background***
  - **FCRA concerns . . . some open reporting agency Q's**
    - **"search for references" class action dismissed – *Sweet v. Linkedin*, No. 14-cv-04531 (N.D. Cal. 4/4/15)**
    - **FTC, *Background screening reports … Just saying you're not a consumer reporting agency isn't enough* (1/10/13)**
  - **Seems like many cos. (and universities) are surfing . . .**
    - ***No. of Employers Passing on Applicants Due to Social Media Posts Continues to Rise*, CareerBuilder (6/26/14)**
    - **BUT EEOC Classifications still in force**

III. Background Checks *(c't'd)*



- **What about asking applicant for:**
  - **Login credentials to view all content?**
  - **Shoulder-surfing?**
    - ***See* Paper at 26-27 & 36**
    - ***Police agencies want access to applicants' social-media passwords*, SF Chron (9/2/14)**

III. Background Checks *(c't'd)*

- **Login Credentials** *(c't'd)*
  - **21: States' Login/Password Bans, *e.g.*:**
    - **9: new ones in last year: CT (10/1/15); LA (8/1/14); MT (4/23/15); NH (9/30/14); OK (11/1/14); RI (6/30/14); TN (1/1/15); VA (7/1/15); WI (4/10/14)**
    - **MOST: expressly apply to state & local gov't**
    - **≥ 8: seem to prohibit "shoulder surfing"**
    - **≥ 13: educational institutions – compiled *here***
    - ***See* this NCSL compilation of 2012-15 laws AND ≥ 11: 2015 bills (new law *or* amendment)**

IV. "Off-Duty" Activities In Web Content

- **Other new twists on old topics, *e.g.*:**
  - **Punishing for Off-Duty activities?**
    - **State statutory rules still apply**
    - **But, at least for public employees, so do codes of conduct and policies . . . and . . .**

IV. "Off-Duty" Web Activities *(c't'd)*

- **Newer topics/questions . . . .**
- **Who owns a Departed Employee's:**
  - **Twitter handle/account?**
  - **LinkedIn "connections"?**
    - ***Cellular Accessories For Less v. Trinitas*, 2014 WL 4627090 (C.D. Cal. 9/16/14) (fact questions for jury)**

IV. "Off-Duty" Web Activities *(c't'd)*

- **Newer issues** *(c't'd)*

- **Recent viable SCA claim regarding accessing employee's social media accounts while she on medical leave**

  - ***Maremont v. Susan Fredman Design Group*, 2014 WL 812401 (N.D. Ill. 3/3/14)**

V. Compliance Basics

- **KUMBAYA?!**

- **Clear, well-thought-out language regarding which multiple constituencies have weighed in . . .**
- **Compliance's "3 E's" = Establish/Educate/Enforce (Nancy Flynn, ePolicy Institute, as discussed here)**

V. Compliance *(c't'd)* – InfoSec Tips

- **Diagnoses of Causes of:**
  - **OPM Breach**
    - **NEW!** ***Moving Forward; How Victims Can Regain Control & Mitigate Threats in the Wake of the OPM Breach*****, INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY (8/19/15)**
    - **Congressional Research Services (CRS),** ***Cyber Intrusion into U.S. Office of Personnel Management: In Brief*** **(7/17/15)**
  - **Anthem Breach**
    - **Eduard Kovacs,** ***Industry Reactions to Anthem Data Breach*** **(Security Week 2/6/15)**
    - **Joseph Conn,** ***Legal liabilities in recent data breach extend far beyond Anthem*****, ModernHealthcare (2/23/15)**
  - **Sony Breach**
    - **Brownstone,** ***Data Breaches: Proactive Prevention and Reactive Remedies*****, at Slides 7-12, AudioSolutionz (5/14/15)**

V. Compliance *(c't'd)* – InfoSec Tips

- **Proactive-Prevention Tips** *(c't'd)*
  - **Brownstone, *Data Breaches: Proactive Prevention . . .*, at Slides 35-46, AudioSolutionz (5/14/15)**
  - **NASCIO's "Capitals in the Clouds" series includes:**
    - ***Part IV – Cloud Security: On Mission and Means*** **(12/19/12 & 6/12/15)**
  - ***Compare* this article:**
    - **Neal Ungerleider, *Why State and Local Governments Are Increasingly Embracing GitHub*, Route Fifty (7/29/15) (LINK FIXED)**

Conclusion/ Questions

- *Q&A*
- **Robert D. Brownstone**
  - Blog ("IT Law Today")
  - Bio | Biblio (articles, press & speeches, Oh My!)
  - Twitter ("@eDiscoveryGuru") | Facebook | LinkedIn | Google+
  - 650.335.7912 or rbrownstone@fenwick.com

- **Please visit home pages for F&W's EIM, Privacy/InfoSec & Employment Groups**

THESE MATERIALS ARE MEANT TO ASSIST IN A GENERAL UNDERSTANDING OF CURRENT LAW AND PRACTICES.

THEY ARE NOT TO BE REGARDED AS LEGAL ADVICE.

THOSE WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.