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

32nd Annual Employment Law Briefing

February/March 2013 – Vail, CO & Las Vegas, NV

The eWorkplace – Social-Media, Privacy & Information-Security Policies

Robert D. Brownstone, Esq.*

---

* *Robert D. Brownstone* is the Technology & eDiscovery Counsel and Co-Chair of the Electronic-Information-Management (EIM) Practice Group at *Fenwick & West LLP*. He advises clients on information-security, privacy, eDiscovery, EIM and retention/destruction policies and protocols.

A nationwide advisor, speaker and writer on many law and technology issues, Bob is frequently quoted in the press as an expert on electronic information.

He also has been teaching Electronic Discovery Law & Process classes at multiple law schools for the past few years.

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

The eWorkplace – Social-Media, Privacy & Information-Security Policies

Materials – TABLE OF CONTENTS

PAGE

PAPER

APPENDICES

TABLE OF CONTENTS

Page

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

Page(s)

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

I. INTRODUCTION – THE MODERN LANDSCAPE[1]

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.[2] 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.[3] In this context, a single negligent or malicious employee can cause truly irreparable harm.

Employers now have many more legitimate reasons to monitor their employees' electronic communications in the workplace.[4] While employers, in pursuing legitimate objectives, may make various intrusions into their employees' privacy, there are nevertheless some limitations on what employers may do.

Moreover, 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. 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) <http://traffic.libsyn.com/legalcurrent/LegalCurrent_April2012.mp3>.

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 and more pivotal in litigation and in the court of public opinion. Examples of well-known figures laid low include: **Anthony Weiner** in the junk-mail tweets situation, Steven Levy, *How Early Twitter Decisions Led to Anthony Weiner's Dickish Demise*, Wired (June 13, 2011) <http://www.wired.com/epicenter/2011/06/twitter-follow-weiner-dickish/all/1>; **Rupert Murdoch**'s and some of Scotland Yard's highest-ranking police

---

[1] The author especially thanks his current colleagues Sheeva J. Ghassemi-Vanni and Sebastian Kaplan and Marion Miller for their invaluable work on various 2010, 2011 and 2012 revisions of this White Paper. The author also thanks his current colleagues Allen Kato, Dan McCoy, Ilana Rubel, Saundra Riley, Michael Sands, Victor Schachter and Dan Ko Obuhanych for their contributions of prior content on which parts of this White Paper are based.

[2] *See* Robert D. Brownstone, *eWorkplace Policies – Social-Media, Privacy & Internet-Security* (Mar. 2012), at 1-3 (.pdf pp. 6-8) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=6> (hereafter "Brownstone eWorkplace II").

[3] Nielsen, *Social Media Report Q3 2011* (Sep. 8, 2011) <http://blog.nielsen.com/nielsenwire/social/>.

[4] For some startling actual numbers (not a survey), see Palo Alto Networks (PAN), *Application & Threat Research Center* (Dec. 2011) <paloaltonetworks.com/researchcenter/reports/>.

officers in the News of the World phone-hacking scandal;[5] **ex-CIA Director David Petraeus**;[6] and former Puerto Rico Legislature President **Robert Arango**.[7]

Recent examples of "loose lips" in various settings include: **Whole Foods CEO John Mackey** (of sock-puppeting notoriety many years ago), Bonnie Kavoussi, *Whole Foods CEO John Mackey Says He Regrets Comparing Obamacare To 'Fascism,'* Huffington Post (Jan. 17, 2013) <www.huffingtonpost.com/2013/01/17/whole-foods-fascism_n_2496603.html>; **Netflix CEO Reed Hastings**' public post on Facebook, Steven M. Davidoff, *In Netflix Case, a Chance to Re-examine Old Rules*, N.Y. Times (Dec. 11, 2012) <http://dealbook.nytimes.com/2012/12/11/in-netflix-case-a-chance-for-the-s-e-c-to-re-examine-old-regulation/>; Joe Mont, *SEC Didn't 'Ile' Netflix CEO's Boastful Facebook Post*, Compliance Week (Dec. 7, 2012) <www.complianceweek.com/sec-didnt-like-netflix-ceos-boastful-facebook-post/article/271779/>; Michael H, Newman, *Are Facebook posts fair disclosure? From the SOX Up* (Dec. 6, 2012) <www.fromthesoxup.com/public-disclosure/are-facebook-posts-fair-disclosure/>; and **New Orleans federal prosecutors** who posted about an ongoing case, Sari Horwitz, *New Orleans U.S. attorney resigns amid scandal over anonymous online postings*, Wash. Post <http://shorl.com/trefrevisufojy>.

---

[5] *See, e.g.,* David Leigh and Nick Davies, *The 'For Neville' email: two words that could bring down an empire*, Guardian (July 22, 2011) <www.guardian.co.uk/media/2011/jul/22/for-neville-email-empire>. *See also* Juan Carlos Rodriguez, *News Corp. Settles Phone Hacking With Fergie, 16 Others*, Law360 (Feb. 28, 2013) <http://www.law360.com/privacy/articles/414011 >; Joe Mont, *News Corp. Hacks $57 Million From Revenue Amid Scandal*, Compliance Week (Aug. 9, 2012) <http://www.complianceweek.com/news-corp-hacks-57-million-from-revenue-amid-scandal/article/254084/>; John F. Burns & Ravi Somaiya, *Murdoch Resigns From His British Papers' Boards*, NY Times (July 21, 2012) <www.nytimes.com/2012/07/22/world/europe/murdoch-resigns-from-british-newspaper-boards.html>; Sarah Lyall and Ravi Somaiya, *Hacking Cases Focus on Memo to a Murdoch*, N.Y. Times (Feb. 11, 2012) <nytimes.com/2012/02/12/world/europe/a-2008-e-mail-at-the-heart-of-a-hacking-scandal.html?pagewanted=all> (linking to key email string at <http://www.parliament.uk/documents/commons-committees/culture-media-sport/PH%2050%20Letter_from_Linklaters_to_Chairman_12_Dec_2011.pdf>); Lisa O'Carroll and Dan Sabbagh, *News International pays out but faces further phone-hacking claims*, UK Guardian (Feb. 8, 2012) (58 settlements to that point; six more cases filed; and 50 more anticipated) <guardian.co.uk/media/2012/feb/08/news-international-phone-hacking-claims?newsfeed=true>.

[6] *See, e.g.,* Hanni Fakhoury, *2012 in Review: Steps in the Right Direction for Email Privacy*, EFF (Dec. 26, 2012) <http://www.eff.org/deeplinks/2012/12/2012-review-steps-right-direction-email-privacy>; Nicole Perlroth, *Trying to Keep Your E-Mails Secret When the C.I.A. Chief Couldn't*, N.Y. Times (Nov. 16, 2012) <http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html?pagewanted=all>; Matthew J. Schwartz, *Petraeus Fallout: 5 Gmail Security Facts*, InformationWeek (Nov. 13, 2012) <http://www.informationweek.com/security/privacy/petraeus-fallout-5-gmail-security-facts/240124937>; Ryan Gallagher, *Instead of "Dead Dropping," Petraeus and Broadwell Should Have Used These Email Security Tricks*, Slate (Nov. 13, 2012) <http://www.slate.com/blogs/future_tense/2012/11/13/petraeus_and_broadwell_should_have_used_pgp_encryption_and_tor_not_dead.html>; Chris Soghoian, *Surveillance and Security Lessons From the Petraeus Scandal*, ACLU (Nov. 13, 2012) <http://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal>; Perry L. Segal, *eDiscovery 101: Petraeus was Done In by Gmail Metadata - Someone Else's!*, e-Discovery Insights (Nov. 12, 2012) <http://www.ediscoverycalifornia.com/insights/2012/11/ediscovery-101-petraeus-was-done-in-by-gmail-metadata-someone-elses.html>.

[7] RT, *Anti-gay Senator caught on all-gay dating site* (Aug. 29, 2011) <http://rt.com/usa/news/senator-arango-grindr-puerto-379/>.

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.[8] Employees' emails can result in bad publicity when attempted smear campaigns against competitors or rivals backfire in large part because the efforts were memorialized in batches of emails.[9] Knowledge of, and indifference to, inappropriate conduct are often memorialized as well.[10] In harassment or discrimination cases, one or two explicit messages can bolster other evidence of hostile environment or discrimination.[11] 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.[12]

---

[8] Brownstone eWorkplace II, supra note 2, at 4 (.pdf p. 9) @ note 16 and accompanying text <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=9>. *See also* Tresa Baldas and Jim Schaefer, *Victor Mercado plea deal a boost for U.S. prosecutors in Kwame Kilpatrick trial*, Detroit Free Press (Nov. 6, 2012) <freep.com/article/20121106/NEWS0102/311060067/Victor-Mercado-plea-deal-a-boost-for-U-S-prosecutors-in-Kwame-Kilpatrick-trial>; M. L. Elrick & Tresa Baldas, *Corruption Case Against Former Mayor Builds With 369k Texts*," WLTX (May 30, 2012) (yet another development in long saga of Detroit ex-Mayor Kwame Kilpatrick) <wltx.com/news/national/article/188899/142/Corruption-Case-Against-Former-Mayor-Builds-With-369k-Texts>.

[9] Brownstone eWorkplace II, supra note 2, at notes 17-18 and accompanying text.

[10] *Id.* at note 19 and accompanying text.

[11] For older situations/cases, *see* Brownstone eWorkplace II, supra note 2, at 5 (.pdf p. 10) and notes 23-24 and accompanying text. <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=10>.

[12] *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) <docs.justia.com/cases/federal/district-courts/puerto-rico/prdce/3:2008cv02408/71930/61/0.pdf?1284361309>; *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) <leagle.com/xmlResult.aspx?page=13&xmldoc=In%20CACO%2020120209057.xml&docbase=CSLWAR3-2007-CURR&SizeDisp=7> (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>). S*ee also* 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>.

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.[13]

a. Internet Activity

Employee Web-surfing can entail visiting pornographic websites, not only cutting into productivity but also potentially creating a hostile work environment and/or criminal liability for knowing possession of contraband. Web activity can also cause serious security breaches for employers.[14] Other lurking potential dangers include phishing and/or whaling schemes[15] as well as e-mail messages containing malware and/or links to malicious websites. Employees' use of social networking sites increases employees *and* employers' vulnerability to malware.[16]

---

[13] *See generally* the lists at pp. 15 and 17 of <nascio.org/publications/documents/NASCIO-SocialMedia.pdf>. In terms of pure negligent use of email, *see Kamps v. Baylor Univ.*, No. A12 Civ. 657 LY, Complaint (W.D. Tex. July 19, 2012) <http://pdfserver.amlaw.com/tx/kampscomplaint.pdf > OR <https://ecf.txwd.uscourts.gov/doc1/181110204153>. *See also* Karen Sloan, *Baylor's accidental doc dump provides grist for bias suit*, Nat'l L.J. (July 25, 2012) <www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202564381624&slreturn=20120706135520>.

[14] Brownstone eWorkplace II, supra note 2, at 5 (.pdf p. 10) @ notes 23-24 and accompanying text. <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=10>. NASA recently experienced a set of security breaches when multiple unencrypted stolen laptops exposed personally identifiable information (PII) on NASA employees, NASA contractors and employees thereof and Kennedy Space Center employees. Rainey Reitman, *NASA's Data Valdez: Thousands of Employees' Personal Information Compromised in Embarrassing Data Breach*, EFF (Nov. 29, 2012) <http://www.eff.org/deeplinks/2012/11/nasas-data-valdez-thousands-employees-personal-information-compromised>; *Losing in Court, and to Laptop Thieves, in a Battle With NASA Over Private Data*, N.Y. Times (Nov. 28, 2012) <http://www.nytimes.com/2012/11/29/technology/ex-nasa-scientists-data-fears-come-true.html>; NASA HQ, *Agencywide Message to All NASA Employees: Breach of Personally Identifiable Information (PII)*, SpaceRef (Nov. 13, 2012) <http://spaceref.com/news/viewsr.html?pid=42609>. Ironically, some of the compromised information had been gathered in background checks, the legality of which had been challenged all the way up to the United State Supreme Court. *Nelson v. NASA*, 1131 S. Ct. 746 (Jan. 19, 2011) (questions in civil service questionnaire as to illegal-drug use) <http://www.supremecourt.gov/opinions/10pdf/09-530.pdf>, as discussed at Brownstone eWorkplace II, supra note 2, at 40-41 (.pdf pp. 45-46) @ notes 170-77 and accompanying text. <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=45>.

[15] Meredith Levinson, *How to Tell if an Email is a Phishing Scam,* PC World (Apr. 10, 2012) <http://www.pcworld.com/printable/article/id,253552/printable.html>.

[16] *See* Kashmir Hill, *You May Not Want To Check Facebook At Work Today*, Forbes (Nov. 15, 2011) <http://www.forbes.com/sites/kashmirhill/2011/11/15/you-may-not-want-to-check-facebook-at-work-today/>. *See also* Brownstone eWorkplace II, supra note 2, at 6 (.pdf p. 11) @ note 26 and accompanying text <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=11>.

b. Posts on Blogs, Wikis, Social Networking Sites, etc.

i. Day-to-day Issues

The various 21st century platforms mentioned in Section I above raise many potential legal liability issues. In addition to chatrooms, Web surfing, and "blogs," the past few years have seen extraordinarily prolific use of smartphones and social-networking.[17]

As to social-networking sites (SNS) sites and applications, 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.[18] In addition, employees' posts may also result in direct organizational liability under: Federal antitrust laws; Federal securities laws; FINRA broker standards; FTC online-advertising guidelines as to endorsements and testimonials; and/or Federal Drug Administration regulations as to prescription-drug advertising.[19]

The Web 2.0 world 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.[20] Throughout the ensuing (sub-)sections of this Paper (and when reviewing the samples linked from 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.

As to the public sector, tweets on Twitter long ago became *de rigeur* for legislators, legislatures' committees, etc. *See, e.g.,* Sensei Enterprises, *PENTAGON OKS SOCIAL- MEDIA ACCESS*, Bytes in Brief (Apr. 4, 2010) <http://web.archive.org/web/20101129151347/http://senseient.com/publications/bytes/html/april_2010.html> (linking to <www.defense.gov/NEWS/DTM%2009-026.pdf>); Congressional Research Service, *Social Networking and Constituent Communications: Member Use of Twitter During a Two-Month Period in the 111th Congress* (Feb. 3, 2010)

---

[17] Brownstone eWorkplace II, supra note 2, at 6 (.pdf p. 11) @ notes 27-29 and accompanying text <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=11>.

[18] *Id.* at notes 30-33 and accompanying text.

[19] *Id.* at 7 (.pdf p. 12) @ notes 34-38 and accompanying text <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=12>. *See also* Joe Mont, *Did Netflix CEO's Facebook Post Violate SEC Disclosure Rules?*, Compliance Week (July 10, 2012) <http://www.complianceweek.com/did-netflix-ceos-facebook-post-violate-reg-fd/printarticle/249416/>; Robert Berry, *The Tweet That Killed The Company*, That Audit Guy (July 9, 2012) (prior to an earnings release, former CFO of Francesca's Collections tweeted: "Board meeting. Good numbers=Happy Board.") <http://www.thatauditguy.com/the-tweet-that-killed-the-company/>.

[20] *Id.* at 7-8 (.pdf pp. 12-13) @ notes 39-41 and accompanying text.

<http://assets.opencrs.com/rpts/R41066_20100203.pdf>; Fed. CIO Council, *Guidelines for Secure Use of Social Media by Federal Departments and Agencies* (Sep. 17, 2009) <cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf>; LLRX, *Government Domain: Tracking Congress 2.0, LLRX* (Aug. 31, 2009) <www.llrx.com/columns/govdomain42.htm>. For some public employees, social media activity presents unique problems: for example, judges and attorneys using social media should be aware of special considerations. For a general discussion of these issues, see, Dahlia Lithwick and Graham Vyse, *Tweet Justice: Should Judges be using Social Media?* (April 30, 2010) <www.slate.com/articles/news_and_politics/jurisprudence/2010/04/tweet_justice.html>.[21]

Some school districts are imposing new guidelines to ban private conversations between teachers and students on social media sites. These new regulations are often based on a concern about "boundary-crossing relationships with students." Jennifer Preston, *Rules to Stop Pupil and Teacher From Getting Too Social Online*, The New York Times (Dec. 17, 2011) <http://www.nytimes.com/2011/12/18/business/media/rules-to-limit-how-teachers-and-students-interact-online.html>.

Other governmental social-media initiatives include: municipalities' inexpensive demographics assessments via Facebook, Lea Deesing, *Social Media for Government Agencies* (Aug. 8, 2012) <http://www.publicceo.com/2012/08/social-media-for-government-agencies/>; and the federal agency rulemaking process, Cary Coglianese,

---

[21] For a discussion of issues related to judges' use of social media, including updates on varying ethics advisory opinions in different states, see Michael Crowell, *Judicial Ethics and Social Networking Sites*, UNC School of Government (revised August 2012), <http://www.sog.unc.edu/sites/www.sog.unc.edu/files/Judges%20social%20networking%20Aug%2012.pdf>. Among ethics opinions, there is a consensus building that judges may join social networks, but that judges should also be aware that social media use creates opportunities for *ex parte* communication that judges should avoid. Just as judges must avoid ties to organizations that may appear before the court and organizations that discriminate in the physical world, judges should be aware of the same issues on social media sites. *Id.* at 7-8. One issue about which there is not consensus is whether judges may accept lawyers as friends on a social network. *Id.* at 8.

Attorneys must also be careful with their use of social media. The New York City Bar Association's Formal Opinion 2012-2 examines whether ethical restrictions apply to attorneys who use search engines or social media websites for the purpose of researching jurors. The opinion cautions attorneys to understand the technology at issue, refrain from engaging in deception to gather information, and promptly report any discoveries of juror misconduct that are gleaned from the research. *Formal Opinion 2012-2: Jury Research and Social Media* <http://www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-formal-opinion-2012-02>. For analysis of that opinion, see Mara E. Zazzali-Hogan, *Attorneys' Use of Social Media to Research Jurors – Another Ethical Land Mine*, E-Discovery Law Alert, June 20, 2012 ("when attorneys use social media websites to research jurors, they have "*arguably* 'communicated' with the juror" if a juror receives an automated message. (Emphasis added). Similarly . . . attempts to research a juror "*might* constitute a prohibited communication even if inadvertent or unintended." Consequently, until a clear pronouncement is made in any jurisdiction, attorneys should routinely sharpen their social media researching skills and their familiarity with the technology, privacy settings and policies of a website if they intend to use that medium to research jurors.") <http://www.ediscoverylawalert.com/2012/06/articles/legal-decisions-court-rules/attorneys-use-of-social-media-to-research-jurors-another-ethical-land-mine/>.

Federal Agency Use of Electronic Media in the Rulemaking Process, U. of Pa., Report to the Administrative Conference of the United States (July 17, 2011) <acus.gov/wp-content/uploads/downloads/2011/08/Coglianese-Report.pdf>. Indeed anyone can now *instantly* become a publisher; and also there is a very good chance that any publicly available Web 2.0 page will be readily findable by standard web search engines and/or archived online even when it has been removed by the original author.[22] Individuals' lack of facility with the ever-changing privacy settings 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: tagging of photos and videos with the names of co-workers and customers; [23] and 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. [24] Thus, in turn, employers' risks of damaging disclosures have thus greatly increased at the same time as their ability to control content has decreased.

Significantly, note that deciding whether to allow employees to use social-media at work is not just an all-or-nothing question due to a growing tool set enabling a more granular approach.[25] In addition, entities such as universities with big sports programs are apparently retaining service providers who monitor student-athletes' tweets for risky content.[26] In addition, those interested in the growing body of social-media ethical prohibitions as to lawyers, jurors and judges should use Appendix D.

---

[22] *Id.* at 8-9 (.pdf pp. 13-14) @ notes 42-45 and accompanying text. <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=13>.

[23] *Id.* at 9 (.pdf p. 14) @ notes 46-48 and accompanying text. <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=14>.

[24] Heather M. Sager, *Why Can't We Be 'Friends'?* Recorder (July 27, 2012) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202564234498>; Tresa Baldas, *Lawyers warn employers against giving glowing reviews on LinkedIn*, Nat'l L.J. (July 6, 2009) <http://tinyurl.com/Baldas-LinkedIn-NLJ-7-6-09> (LEXIS login needed to access this article); LinkedIn, *"Who's Viewed Your Profile" - Overview and Privacy* (Mar. 7, 2011) <http://help.linkedin.com/app/answers/detail/a_id/42>; LinkedIn Settings, "Select what others see when you've viewed their profile" (see screenshot in Slide 14 of Appendix E) <linkedin.com/settings/?tab=profile&modal=nsettings-wvmp-visibility> (last visited Apr. 17, 2012).

[25] *See, e.g.,* NSS Labs, 2012 Next Generation Firewall Security Value Map™ (Mar. 1, 2012) <http://www.paloaltonetworks.com/literature/research/NSS-Labs-NGFW-SVM-2012.pdf>; Ashlee Vance, *Palo Alto Networks takes firewalls to next level*, Bloomberg Businessweek (Oct. 23, 2011) <sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/10/23/BULH1LKCDV.DTL&type=printable>; Klint Finley, *Read-Only Facebook Coming to Your Company?* ReadWrite Enterprise (June 8, 2010) <http://www.readwriteweb.com/enterprise/2010/06/read-only-facebook-coming-to-y.php>. *See also* U.S. Navy Slideshare, *What's the deal with Google+?* (7/29/11) <http://www.slideshare.net/USNavySocialMedia/whats-the-deal-with-google>.

[26] Pete Thamel, *Tracking Twitter, Raising Red Flags*, N.Y. Times (Mar. 30, 2012) <nytimes.com/2012/03/31/sports/universities-track-athletes-online-raising-legal-concerns.html> (discussing Varsity Monitor <http://varsitymonitor.com/>).

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

A. General Guidelines

B. Specific Guidelines

1. Employer-Sponsored Social-Networking Pages, Wikis, Blogs, etc.

2. Personal Social-Networking Pages, Wikis, Blogs, etc.

---

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

Some employees' social-media postings, though, may end up being beneficial to employers. Indeed, in litigation, loose-lipped postings might be a discovery gold-mine for an employer-Defendant. Electronic discovery (eDiscovery) pertaining to emails and electronic documents has been commonplace in litigation for some time; however, posts, tweets, texts and "private" Facebook and MySpace messages are now becoming entrenched additional targets of production requests and subpoenas.[27] In response to search warrants and court orders, social media companies can provide content and

[27] Brownstone eWorkplace II, supra note 2, at 10-13 (.pdf p. 15-18) @ notes 49-60 and accompanying text <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=15>. Moreover, anyone using a mobile device leaves a "vast digital footprint." Kevin L. Nichols, *The Evolving Trends of Social Media eDiscovery: Tidbits from the Masters Series 2012 in San Francisco*, eDiscovery Journal (Apr 23, 2012) (reporting on Neal Lawson's hypothetical of a day-in-the-life usage of Groupon, Foursquare, Facebook, GroceryIQ and Yelp) <http://ediscoveryjournal.com/2012/04/the-evolving-trends-of-social-media-ediscovery/>. *See also* Jennifer Walrath and Gil Keteltas, *Is Social Media Discoverable? Stick to the Basics*, Discovery Advocate (March 26, 2012) <www.discoveryadvocate.com/2012/03/26/is-social-media-discoverable-stick-to-the-basics-part-i-relevance/>; Redgrave & Johnson, *Social Media Case Alerts*, Redgrave LLP (Feb. 24, 2012) <redgravellp.com/userfiles/files/SocialMediaCaseAlertSummary_Jonathan_Redgrave_Kathy_Johnson.pdf>.

metadata from users' social media accounts.[28]

While some aspects of social networking websites remain cloaked in privacy, these modern venues are now unquestionably part of the discovery milieu, including in employment cases.[29]

In an Oregon federal case, the court found "no principled reason to articulate different standards for the discoverability of communications through email, text message, or social media platforms."[30] In addition, a federal court in Pennsylvania noted that the use of social media evidence in discovery is a two-way street. *Quagliarello v. Dewees*, 2011 WL 3438090 (E.D. Pa. Aug. 4, 2011) ("Memorandum re: Motions in

---

[28] Last Fall, a New York criminal court judge ordered Twitter to produce a sealed document containing tweets and data from an Occupy Wall Street protester's Twitter account. In addition to the defendant's tweets, prosecutors sought information about the IP address from which he had logged in, direct messages and deleted messages, as well as how long each login lasted, including dates, times and possible location information. Megan Geuss, *Twitter Hands Over Sealed Occupy Wall Street Protester's Tweets*, ArsTechnica (Sept. 14, 2012) <http://arstechnica.com/tech-policy/2012/09/twitter-hands-over-occupy-wall-street-protesters-tweets/>. *Compare Juror No. One v. Superior Court (Royster)*, 206 Cal. App. 4th 854, 142 Cal. Rptr. 3d 151, 153 (Cal. App. 3 Dist. May 31, 2012) (upholding "order requiring [j]uror . . . to execute [SCA] consent form . . . authorizing Facebook to release to the court for in camera review all items he posted during [criminal] trial") <http://www.courts.ca.gov/opinions/documents/C067309.PDF>.

[29] *See generally* the partial compilation of cases in Appendix B. As to the employment context in particular, *see, e.g.*, *E.E.O.C. v. Original Honeybaked Ham Co. of Georgia*, 2012 WL 5430974 (D. Colo. 11/7/12) (broad discovery as to class of 20+) <http://articles.law360.s3.amazonaws.com/0393000/393985/HBH.pdf >; *E.E.O.C. v. Simply Storage Management, LLC,* 270 F.R.D. 430, 434 (S.D. Ind. May 11, 2010) (social-networking site – a/k/a "SNS" – "*content is not shielded from discovery simply because it is 'locked' or 'private'*[;] and "*SNS content must be produced when it is relevant to a claim or defense in the case*") <http://www.iediscovery.com/files/Simply_Storage.pdf>; *Nguyen v. Starbucks Coffee Corp.*, 2009 WL 4730899, 92 Empl. Prac. Dec. ¶ 43,761 (N.D. Cal. Dec. 7, 2009) (granting summary judgment to employer/Defendant where employee/Plaintiff's blog entry had contained threats against employer and co-workers) <ecf.cand.uscourts.gov/doc1/03516287723>; *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007) <https://ecf.nvd.uscourts.gov/doc1/11511167020> (discussed in depth at Brownstone eWorkplace II, supra note 2, at 11 (.pdf p. 16) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=16>).

[30] *Robinson v. Jones Lang LaSalle Americas, Inc.*, 2012 WL 3763545 (D. Ore., Aug. 29, 2012) <www.ediscoverylaw.com/uploads/file/Robinson%20v%20Jones%20Lang%20LaSalle.pdf>. *See also* K&L Gates, *Case Summary: Robinson v. Jones Lang LaSalle* (Sep. 6, 2012) <ediscoverylaw.com/2012/09/articles/case-summaries/court-sees-no-principled-reason-to-articulate-different-standards-for-the-discoverability-of-communications-through-email-text-message-or-social-media-platforms/>. *But see* Abigail Rubenstein, *Courts Struggle to Lay Out Social Media Discovery Limits*, Law360 (Sept. 20, 2012) (summarizing judge's rejection of employer's bid for broad access to former employee's social networking posts in *Danielle 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) <gibbonslaw.com/files/1349899536.pdf>; and noting that "[t]hough attorneys expect that the courts will eventually reach a consensus, the issue is likely to remain hotly contested for now as courts try to determine what is best without many decisions to look to for guidance") <law360.com/articles/379673/courts-struggle-to-lay-out-social-media-discovery-limits>.

Limine") <http://www.technolawyer.com/litigationworld/d/quagliarello080412.pdf>. In particular, that court not only agreed with a Defendant that some social media photographs of Plaintiff could be relevant to her emotional distress claim, but also found that Plaintiff could rebut social media evidence on redirect by introducing other social media photographs from the same time period. Yet another decision rejected a hearsay objection to the introduction of Facebook messages.[31]

Moreover, a Federal District Court in New York acknowledged that privacy rights often must give way during the discovery phase in employment lawsuits, in New York required a plaintiff to produce non-public postings from her Facebook account. In *Reid v. Ingerman Smith LLP*, 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012) <http://docs.justia.com/cases/federal/district-courts/new-york/nyedce/1:2012cv00307/326380/33/0.pdf?ts=1356693028>, a legal secretary sued her former law firm employer, alleging that one of her former supervisors subjected her to same-sex harassment. Because Plaintiff sought emotional distress damages, the employer sought to discover private postings from plaintiff's Facebook account on the grounds that publicly available postings revealed information contradicting plaintiff's claims of mental anguish. The court held that certain private postings — including postings about plaintiff's social activities — were discoverable, as they may contain relevant information regarding plaintiff's emotional state.

Another front on which to look for new developments is discovery of postings on *intra-company*, *i.e.*, "enterprise social networking," platforms, such as Yammer (just acquired by Microsoft) and Chatter. *See generally* Ashlee Vance, *Yammer, Chatter, Hot Water*, Bloomberg Bus. Week (Apr. 28, 2011) (quoting Robert Brownstone) <http://www.businessweek.com/magazine/content/11_19/b4227031833107.htm>.

Note also that, aside from social-media postings, last year some cutting edge eDiscovery law has been developed in the course of a couple employment discrimination cases. *See, e.g., Pippins v. KPMG , LLP*, 279 F.R.D. 245 (S.D.N.Y. Feb. 3. 2012) (in absence of Defendant's cooperation in meet/confer, ordering continued preservation of thousands of workers' hard drives of workers in class action alleging misclassification of hourly workers as exempt from overtime pays) <http://www.ediscoverylawalert.com/uploads/file/Pippins%20ii.pdf>; *Moore v. Publicis Groupe*, --- F.Supp.2d ----, 2012 WL 607412 (S.D.N.Y. Feb. 24, 2012) (court-ordered protocol as to use of technology-assisted review, a/k/a "predictive coding: in phase one pre-certification discovery in putative class-action alleging gender discrimination) <http://www.ediscoverylaw.com/uploads/file/Da%20Silva%20Moore%20Opinion.pdf>.

Some decisions have also addressed the issue of the authentication of social media content in eDiscovery. For example, compare *Griffin v. State*, 19 A. 3d 415 (Md. Ct. App. 2011) (birth date and photo insufficient to authenticate printout of MySpace profile) <mdcourts.gov/opinions/coa/2011/74a10.pdf>[32] with *Tienda v. State*, 358 S.W.3d 633 (Tex.

[31] *People v. Oyerinde*, 2011 WL 5964613 (Mich. Ct. App. Nov. 29, 2011) (Facebook messages not hearsay and thus admissible as party admission because Defendant sent them to another person) <publicdocs.courts.mi.gov:81/OPINIONS/FINAL/COA/20111129_C298199_51_298199.OPN.PDF>.

[32] "The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language. … [O]ther courts, called upon to consider authentication of electronically stored information on social networking sites, have suggested greater scrutiny because of the heightened possibility for manipulation by other than the true user or poster." *Griffin v. State*, 19 A. 3d 415, 424, citing *Commonwealth v. Williams*, 456 Mass. 857, 926 N.E.2d 1162 (2010).

Crim. App. Feb. 8, 2012) (circumstantial evidence sufficient to authenticate MySpace postings) <cca.courts.state.tx.us/OPINIONS/PDFOPINIONINFO2.ASP?OPINIONID=22068>[33] and *People v. Valdez*, 201 Cal. App. 4th 1429, 1434-1437 (Cal. App. 4th Dist. Dec. 16, 2011) (section on authentication not published) (holding that reasonable trier of fact could conclude from the posting of personal photographs, communications, and other details that the social media profile belonged to the Defendant) <http://shorl.com/pruprynemadetu>.

The author has begun using a powerful program, X1 Social Discovery <http://www.x1discovery.com/socialdiscovery.html>. That tool captures and authenticates from the internet publicly available electronic evidence from, among other sources, social-media sites such as Twitter and Facebook. 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. 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"[34] and multiple other items. X1 Social Discovery can also collect and authenticate the contents of, for example, a Gmail box or a Yahoo mailbox provided the login credentials are available – and have been legally obtained (*see* case law discussed in footnotes 46-47 and accompanying text in Section II(B)(1)(c) below).

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 their predispositions as to a job 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> and, someday soon, in the Twitter archive of public tweets at the Library of Congress.[35]

Moreover, as to any given governmental entity's social-media sites, public records obligations may very well require the archiving and retention of tweets and other posts. *See OMA Request for Review*, 2012 PAC 21667, Ill. A.G. (Oct. 31, 2012) (declining to address citizen's allegation that a Village "violated his freedom of speech by deleting his comments and questions from the Village's Facebook Fan page" in course of address Ill. Open Meetings Act issue as to Village's posting of notices and agendas as to public meetings) <docs.google.com/file/d/0B-50NTfFaSE7ampxaXNsUUVCWms/edit>, which is discussed in Jackie Wernz, *Public Entity Deletes Comments From Facebook Page: The Right Choice?* Franczek

---

[33] Extending the approach used to authenticate other digital content, the court held that MySpace postings were sufficiently linked "such that a reasonable juror could have found that they were created and maintained" by the defendant. The circumstantial evidence, taken as a whole, sufficiently established that the MySpace pages were created and maintained by the defendant.

[34] 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).

[35] Matt Raymond, *How Tweet it Is!: Library Acquires Entire Twitter Archive*, Library of Congress Blog (April 14, 2010) <http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/>. *See also* Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. Times (July 9, 2010) <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all>.

Radelet P.C. (Nov. 30, 2012) <www.lexology.com/library/detail.aspx?g=709ddd1b-33c3-49c1-be3f-b25b2581eb2b>. *See generally* some of the resources linked from Appendix A. *See also* additional public-records resources available from the author.

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.[36] Last year the FTC approved the potential legality of a one-year old start-up company, "Social Intelligence," whose business model includes performing social media background checks on applicants; however, in 2011 the FTC issued warning letters to purveyors of background-screening mobile apps.[37]

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.

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. Key *recent* developments from the past couple years as to those five respective issues are discussed below *seriatim*. For a fuller treatment of the pre-2011 legal standards in these areas, *see* Brownstone eWorkplace II, supra note 2, at 14-36 (.pdf pp. 19-41) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=19> and to the predecessor White Paper (hereafter "Brownstone eWorkplace I") to which it links.

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

a. ECPA (Wiretap & SCA)

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

---

[36] Annie Fisher, *Checking Out Job Applicants on Facebook? Better Ask a Lawyer*, Fortune (March 2, 2011) <http://management.fortune.cnn.com/2011/03/02/checking-out-job-applicants-on-facebook-better-ask-a-lawyer/>. For a discussion about whether requiring applicants to disclose social media login information is illegal, *see* Section III(B)(3) below.

[37] *See* note 93 and accompanying text below.

employer's right to retrieve and read such e-mails.[38] Note, however, 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.[39]

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 Yahoo and Hotmail.[40] Many of these employees may not realize that such

---

[38] *See, e.g., Fraser v. Nationwide Mut. Ins. Co*., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part and remanded in part on other grounds*, 352 F.3d 107 (3d Cir. 2004); *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183 (S.D. Cal. 2008). *See generally* Brownstone, Robert D., 9 *Data Security & Privacy Law, Privacy Litig.* Ch. § 9:29 (West 2012).

[39] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879–80 (9th Cir. 2002); *Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 925–26 (W.D. Wis. 2002). As a practical matter, the employer was given wide latitude by the court to snoop on the employee's website. Yet, in *Fischer* (unlike *Fraser*, where the e-mail message accessed was stored on the employer's server), an employer and its computer consultant accessed plaintiff's private Web-based e-mail account. The court noted, in dicta, that the SCA's legislative history was designed to "cover the exact situation in this case." 207 F. Supp. 2d at 925–26. Nevertheless, to succeed on an SCA claim, Plaintiff also had to show that Defendants obtained, altered, or prevented the employee's authorized access to his e-mail account pursuant to section 2701(a). *Id.* at 926. Because pertinent fact issues existed, summary judgment was denied to Defendants. *Id. Compare 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) <http://law.justia.com/cases/federal/district-courts/california/candce/3:2010cv04700/233056/220>.

But in a non-employment litigation matter, the South Carolina Supreme Court has held that accessing someone's web-based e-mail without his/her permission does not violate the SCA because web-based e-mail – like Gmail or Yahoo Mail – does not meet the definition of electronic storage under the SCA. *Jennings v. Jennings*, --- S.E.2d ----, 2012 WL 4808545 (S.C. Oct. 10, 2012) <http://www.sccourts.org/opinions/HTMLFiles/SC/27177.pdf>. *See* Cyrus Farivar, *Reading Someone's Gmail Doesn't Violate Federal Statute, Court Finds*, ArsTechnica (Oct. 11, 2012) (discussing a split between the South Carolina Supreme Court's *Jennings* decision and existing case law from the Ninth Circuit Court of Appeals) <http://arstechnica.com/tech-policy/2012/10/reading-someones-gmail-doesnt-violate-federal-statute-court-finds/>.

In another case, a juror's posts about an ongoing trial were not protected by the SCA. *Juror No. One v. Superior Court (Royster)*, 206 Cal. App. 4th 854, 142 Cal. Rptr. 3d 151, 153 (Cal. App. 3 Dist. May 31, 2012) <http://www.courts.ca.gov/opinions/documents/C067309.PDF>. There, a juror had posted on Facebook that testimony about cell phone records was so boring he had almost fallen asleep, but testified that he had not read any responses to his posts. A unanimous appellate panel ruled that the SCA offered no protections to Juror No. 1 and ordered him to sign a consent form that would authorize Facebook to forward the posts to the trial judge for *in camera* review. The California Supreme Court in effect upheld the decision in August 2012 by denying review. Scott Graham, *State Justices Clear Path for Judge to Review Juror's Facebook Posts*, The Recorder (August 23, 2012) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202568750336>.

[40] At times, an "e-sabotage" scenario ensues whereby a corporate insider uses a third-party e-mail services to transmit confidential information from his or her employers' computer systems.

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.[41]

In general, however, there is a lot of confusion on the state of the law under the ECPA, in light of Congress' failure to act to bring the statutory provisions in line with modern technologies.[42] Moreover, the issues get even more complicated when foreign citizens' emails and/or other electronic communications are in question.[43]

One last point to keep in mind 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 . *See generally* A. Louis Dorny, *Get Consent and Avoid Sanctions*, Cal. Lawyer (July 2012) (citing the *Royster* SCA juror consent decision discussed in footnotes 28 and 39 above) <callawyer.com/clstory.cfm?eid=923324>. *See also* Slide 11 of Appendix E as to Facebook's "Download Your Information" and Twitter's "Your Twitter Archive."

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

Several recent decisions have each dismissed one or more common-law invasion of privacy claim based on Facebook post(s) by an employee or an employer. *See, e.g., Murdock v. L.A. Fitness Int'l LLC*, 2012 WL 5331224, at *3-*4 (D. Minn. Oct, 29, 2012) (finding allegations based on employer's post-termination Facebook posts "insufficient to state a claim for either intrusion upon seclusion or publication of private facts" or "intentional infliction of emotional distress) <http://docs.justia.com/cases/federal/district-courts/minnesota/mndce/0:2012cv00975/125597/22/0.pdf?1351596764>; *Sumien v. CareFlite*, 2012 WL 2579525, at *3 (Tex. Ct. App. 2 Dist. July 5, 2012) (affirming dismissal of EMT's unlawful termination, intrusion on seclusion and public disclosure claims based on Plaintiff's Facebook posts; Plaintiff's misunderstanding of Facebook settings did not indicate illegal intentional intrusion on part of employer) <http://www.2ndcoa.courts.state.tx.us/opinions/PDFOpinion.asp?OpinionId=23493>; *See also Roberts v. CareFlite*, 2012 WL 4662962 (Tex. Ct. App. 2 Dist. Oct. 4, 2012) (affirming summary judgment dismissing *Sumien* co-worker's seclusion claim <http://www.2ndcoa.courts.state.tx.us/opinions/PDFOpinion.asp?OpinionId=23723>; *Ehling*, infra note 50.

In general, to avoid any arguments premised on a "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.[44]

---

[41] *See*, for example, the "Spector" software package <http://www.spectorsoft.com/>.

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

[43] As to foreign citizens, *see Suzlon Energy Ltd. v. Sridhar [Microsoft]*, 671 F.3d 726 9th Cir. Oct. 3, 2011) (not employer-employee case) <ca9.uscourts.gov/datastore/opinions/2011/10/03/10-35793.pdf>.

[44] *See, e.g.*, the many opinions – including two from the ABA – gathered in Appendix C.

Note, though, that, at times, such arguments have been trumped by attorney-client privilege, where policy language and enforcement practices have not been airtight and thus deemed to give way to public-policy favoring protection of privilege.[45] The outcomes 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.

The various privilege-vs.-TAUP decisions, sometimes hinging on factual circumstances and other times on public-policy, are refreshing recognitions of the role of email in the workplace and in litigation today, and the need of the judicial system to further delineate the standards for adjudication of alleged privacy rights in this area.

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. Such a manual can include a written protocol whereby, once having embarked on a duly authorized investigation or collection, investigation personnel must contact the employer's Legal Department (or outside counsel) as soon as he/she comes across an electronic or hardcopy communication between a current or former employee and that employee's own individual legal counsel.

c. ECPA Limits on Intrusions into Workers' Private Accounts

If there is no actual trail left on an employer's system or computer, then, under several 2009 federal decisions, 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.[46] *See also* an Illinois state court decision interpreting the ECPA, namely *Borchers v. Franciscan Tertiary Province of the Sacred Heart, Inc.*, 2011 IL App (2d) 101257, 962 N.E. 2d 29 (Feb. 28, 2012) (denying summary judgment to employer where supervisor's assistant had accessed Plaintiff's personal AOL email account) <www.state.il.us/court/opinions/AppellateCourt/2011/2ndDistrict/December/2101257.pdf>.[47]

---

[45] *See generally* the decisions and articles gathered in Appendix C.

[46] *See Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199, 209 (4th Cir. 2009) <http://pacer.ca4.uscourts.gov/opinion.pdf/071892.P.pdf>; *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420, at *6, 29 IER Cases 1438 (D.N.J. Sep. 25, 2009) (upholding verdict finding unlawful access where manager pressed hostess to divulge her login and password to employees' invitation-only MySpace group page and then fired her based on her comments therein) <https://ecf.njd.uscourts.gov/doc1/11914223001>; *Brahmana v. Lembo*, 2009 WL 1424438, at *1, *3 (N.D. Cal. May 20, 2009) <http://op.bna.com/pl.nsf/id/dapn-7sfhhx/$File/brahmana.pdf>. *See generally* Brownstone eWorkplace II, supra note 2, at 19-20 (.pdf pp. 24-25) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=24>.

[47] *See also* Jay P. Lechner, *Why You Should Check With Legal Before Searching Employee's Emails*, Nat'l Rev. (Mar. 8. 2012) <http://www.natlawreview.com/article/why-you-should-check-legal-searching-employee-s-emails>.

In contrast to those decisions, however, *see* Section V(B)(1)(a) below for a discussion of a state court appellate decision – *Sitton v. Print Direction, Inc.*, 2011 WL 4669712 (Ga. App. Sep. 28, 2011) <http://caselaw.findlaw.com/ga-court-of-appeals/1594039.html> – that hat approved of an employer's exercise of very broad employer inspection, even extending to a personal webmail account from an employee's own personal bring-to-the-office computer.

In general, the importance of having an explicit pertinent policy in place – establishing the right to monitor and inspect – was buttressed by a couple 2007-08 wide-ranging Stored Communications Act (SCA) Circuit opinions, one employment-related and one not.[48] During 2010, each of those cases – *City of Ontario v. Quon*, 130 S. Ct. 2619 (U.S. June 17, 2010) <http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf> and *United States v. Warshak*, 631 F.3d 266 (6th Cir. Dec. 14, 2010) <www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf> resulted in a ground-breaking Fourth Amendment decision having implications in other contexts. *See* the ensuing sub-section (d)(i) for some details.

In late 2012, two interesting ECPA decisions came down, one finding a violation of Title I of the ECPA (the Wiretap Act), *Shefts v. Petrakis*, 2012 WL 4049484 (C.D. Ill. 9/13/12) (Wiretap Act violated by virtue of covert screen captures of received emails via spyware being an "interception; different result as to text messages) <http://docs.justia.com/cases/federal/district-courts/illinois/ilcdce/1:2010cv01104/49054/248/0.pdf?ts=1347622354> , and the other affirming the dismissal of a claim as not showing a violation of Title II (SCA) of the ECPA, *Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. 12/12/12) (SCA not violated by unauthorized access to data stored on personal cell phone) <www.ca5.uscourts.gov/opinions/pub/11/11-41118-CV0.wpd.pdf>.

d. Constitutional Limits

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

In *Quon,* police officer Jeffrey Quon 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.[49] For a full discussion of the holding of the U.S. Supreme Court in *Quon*, *see* Brownstone eWorkplace II, supra note 2, at 20-24 (.pdf pp. 25-29) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=25>.

---

[48] The non-employment one was *Warshak v. United States*, 490 F.3d 455, 472-73 (6th Cir. 2007) (distinguishing *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) from *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007)) <ca6.uscourts.gov/opinions.pdf/07a0225p-06.pdf>. *See also* Morphy, Erika, *Carving Out New Privacy Rights for E-Mailers*, e-Commerce Times (June 21, 2007 <ecommercetimes.com/story/57953.html>.

[49] *See Employer Violated Employee Privacy by Accessing Personal Text Messages,* Fenwick Emp. Brief (July 10, 2008) <fenwick.com/publications/6.5.4.asp?mid=36&WT.mc_id=EB_071008>, on which this discussion of the *Quon I* Ninth Circuit decision is partially based.

In sum, *Quon*'s enduring lessons for all employers are: be mindful of what one commits to writing; and erect a divide between one's personal and work-related communications. Some post-*Quon* tips for a compliant TAUP for a public or private employer are:

- ***Top Ten Takeaways***
    - 10. Have a clear written policy covering all information created, stored, received or transmitted on or by any system or device provided by the employer
    - 9. Decide whether to extend to all devices supported, or costs -reimbursed, by the employer and make the scope clear:
        - in the written policy;
        - to all supervisors/managers; and
        - to all staff
    - 8. Specify all employer rights, including to:
        - monitor;
        - search;
        - access;
        - inspect; and
        - read
    - 7. Give clear written notice to all employees and covered third parties allowed access to employer systems/networks
    - 6. Be realistic as to "personal use" – strongly consider "limited" or "incidental" exception, but with carve-outs for activity:
        - violating law or any employer policy;
        - interfering with employee's job performance and/or with employer's operations;
        - aims for personal pecuniary gain to the detriment of the employer; or
        - harms any customer/client/constituent or co-worker
    - 5. Train new employees – and periodically retrain experienced ones – on key TAUP provisions, especially re: NoEEPP
    - 4. Train supervisors/managers re: consistent, fair enforcement
    - 3. Do not overreach as to:
        - an employee's own attorney-client privilege; or
        - the illicit obtainment – let alone use – of an employee's personal login/password
    - 2. Provide annual concise reminder summarizing key TAUP provisions
    - 1. Periodically – every two or three years? – review (and revise?) the TAUP so it's: consistent with actual practices; and up-to-date as to current technology, *e.g.,* smartphones and social networking sites.

As to the first two Takeaways – 10. and 9. – the Bring Your Own Device (BYOD) issue has become more and more complicated in recent years. *See, e.g.,* Margaret A. Keane, *The Accidental Cloud* , at 33-52 Strafford (Oct. 16, 2012) <media.straffordpub.com/products/cloud-services-managing-privacy-risks-2012-10-16/presentation.pdf#page=33>*;* Littler Mendelson, *Employee Use of Dual-Purpose Electronic Devices: Legal Challenges for Employers*, Strafford (Sep. 27, 2012) <http://media.straffordpub.com/products/employee-use-of-dual-purpose-electronic-devices-legal-challenges-for-employers-2012-09-27/presentation.pdf>; Cheryl Orr, *Employer's BYOD Dilemma*, Recorder (July 27, 2012) ("[w]ith employees using their personal electronics for business, the contours of expectation of privacy are blurred") <http://www.law.com/jsp/ca/PubArticleFriendlyCA.jsp?id=1202564236638>; Joe Mont, *The Risks and Benefits of Allowing Employee-Owned Devices*, Compliance Week (June 5, 2012) <http://www.complianceweek.com/the-risks-and-benefits-of-allowing-employee-owned-devices/article/243943/>.

For full discussions of the 2010 Fourth Amendment decisions in the non-employment cases of *Warshak III* and *Rehberg v. Paulk*, 611 F.3d 828 (11th Cir. 2010) <ca11.uscourts.gov/opinions/ops/200911897reh.pdf>, *see* Brownstone eWorkplace II, supra note 2, at 24-25 (.pdf pp. 29-30) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=29>. Those two non-workplace decisions may impact the standards in similar future employment disputes as to, among other issues, the discoverability of individuals' emails that reside on the servers of ISP's.

Moreover, in the social-media realm, the analysis of whether a person has a reasonable expectation of privacy is context-dependent. For example, courts may be more likely to find a reasonable expectation of privacy where Facebook posts are restricted[50] or where emails were viewed on a computer designated for personal use.[51] In any event, tor all individuals, whether in the workplace or otherwise, the overarching takeaway from *Quon* and the subsequent social-media decisions is a resounding one: Even though personal, password-protected email accounts are usually safe havens, privacy rights as to cell phones and text messages, especially involving company-issued devices, are quite vulnerable.

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

[50] *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>.

[51] *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) <http://law.justia.com/cases/federal/district-courts/california/candce/3:2010cv04700/233056/220>.

entities, must walk a fine line between enforcing their anti-harassment and computer usage policies, while remaining cognizant of their employees' free speech rights.

In the public sector, First Amendment implications can also arise from employee use of employer-provided email systems, such as in the 2009 Ninth Circuit decision in *Rodriguez v. Maricopa County Cmty. College Dist.*, 605 F.3d 703 (9th Cir. 2009) <ca9.uscourts.gov/datastore/opinions/2010/05/20/08-16073.pdf> (First Amendment defense succeeded based on finding of qualified immunity because "'[t]here is no categorical "harassment exception" to the First Amendment's free speech'"). For a discussion of this decision, *see* Brownstone eWorkplace II, supra note 2, at 24-25 (.pdf pp. 29-30) <*fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=29*>.

Compare Garcetti v. Ceballos (District Attorney "did not speak as a citizen by writing a memo that addressed the proper disposition of a pending criminal case"), 547 U.S. 410, 422 (U.S. 2006) <http://laws.findlaw.com/us/000/04-473.html>, as discussed in Deb McAlister-Holland, *7 Things the First Amendment Doesn't Protect,* Business 2 Community (Feb. 6, 2012) ("[p]ublic speech made in the conduct of their duties by public employees may not be protected")") <www.business2community.com/social-media/7-things-the-first-amendment-doesnt-protect-0129234>. *See also Foley v. Town of Randolph*, 598 F.3d 1, 10 ("under circumstances which indicate that [Town Fire Chief] was speaking as Chief, members of the Board did not violate [his] free speech right when they concluded that it was inappropriate for [him] to address budgetary and staffing issues [at press conference] at the scene of a fatal fire") <http://www.ca1.uscourts.gov/cgi-bin/getopn.pl?OPINION=09-1558P.01A >; *Curran v. Cousins*, 509 F.3d 36, 49 (1st Cir. 2007) (affirming sheriff's department's dismissal of corrections officer based on angry post on union website; "[s]ignificant weight is given to the public employer's 'reasonable predictions of disruption, even when the speech involved is on a matter of public concern.'" (quoting *Garcetti*) <ca1.uscourts.gov/cgi-bin/getopn.pl?OPINION=07-1686.01A>.

But see 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>.

As indicated by some of the below parenthetical summaries, recent years have seen growth in the number of those types of First Amendment decisions involving posts on Facebook or another social media site. And, given the unsettled state of the law, notices of appeal have been filed as to some of the ones cited below. *See, e.g., In re O'Brien*, 2013 WL 132508, at *3-*4 (N.J. A.D. Jan. 11., 2013) (affirming ALJ's finding that "a description of first-grade children as criminals with their teacher as their warden is intemperate and vituperative" supported teacher's discharge by, at a minimum, outweighing any putative First Amendment rights) <http://www.njlawarchive.com/archive/a2452-11.pdf>; *Tatro v. U. of Minnesota*, 816 N.W. 2d 509, 524 (Minn. June 20, 2012) ("affirm[ing] the University's discipline of [Mortuary Science Program student] for Facebook posts that violated [narrowly tailored] academic program rules governing the privilege of access to human cadavers") <http://www.lawlibrary.state.mn.us/archive/supct/1206/OPA101440-0620.pdf>; *Gresham v. Atlanta*, 2011 WL 4601020, at *2, *4 (N.D. Ga. Sep. 30, 2011) (although "Plaintiff [/Police-Officer]'s speech did pertain to an issue of public concern

and thus [wa]s entitled to First Amendment protection," granting summary judgment to Defendants because choice of Facebook personal profile rather than a more public forum militated in favor of superiority of Department's interests "in maintaining solidarity, order, and discipline within the police force, and in maintaining public trust and confidence in its capabilities.") <https://ecf.gand.uscourts.gov/doc1/05515325114>. *See generally* Jack Ryan, *Facebook© and the First Amendment Rights of Police Officers*, PATC Legal & Liability Risk Management Institute (Mar. 21, 2012) <http://www.patc.com/weeklyarticles/print/2012_facebook_first_amendment.pdf>. *See also Mattingly v. Milligan*, 2011 WL 5184283, at *4 (E.D. Ark. Nov. 1, 2011) (summary judgment denied in part where "speech related to a matter of public concern") <http://docs.justia.com/cases/federal/district-courts/arkansas/aredce/4:2011cv00215/85729/26/0.pdf?1320214809>.

A new issue is whether "liking" a Facebook page is protected speech. *Bland v. Roberts*, 2012 WL 1428198 (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") <www.citmedialaw.org/sites/citmedialaw.org/files/04-24-2012-District%20Court%20Opinion%20granting%20Summary%20Judgment.pdf>. The *Bland* District Court decision is now on appeal; and amicus briefs have been filed by the ACLU <http://www.aclu.org/files/assets/bland_v._roberts_appeal_-__amicus_brief_.pdf > and by Facebook <http://docs.justia.com/cases/federal/appellate-courts/ca4/12-1671/18/0.pdf?ts=1344358360>. eDockets for the case are available at <https://ecf.ca4.uscourts.gov/cmecf/servlet/TransportRoom?servlet=CaseSummary.jsp&caseNum=12-1671&incOrigDkt=Y&incDktEntries=Y> (PACER login/password needed) and <http://dockets.justia.com/docket/circuit-courts/ca4/12-1671/>. *See generally* CMLP, *Threats; Bland v. Roberts*, Citizen Media Law Project (6/25/12) <citmedialaw.org/threats/bland-v-roberts>; Ken Paulson, *Is 'liking' on Facebook a right?* USA Today (5/29/12) <http://www.usatoday.com/news/opinion/forum/story/2012-05-29/facebook-twitter-free-speech-social-media/55269614/1>.

In a state such as California, which has a constitutional right to *privacy*, private sector employees may have a tenable constitutional claim. However, as to constitutional *free speech rights*, typically private sector employers are immune from First Amendment claims. *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") <www.gpo.gov/fdsys/pkg/USCOURTS-ohnd-5_11-cv-00399/pdf/USCOURTS-ohnd-5_11-cv-00399-1.pdf>.

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 monitoring of electronic communications, several states have enacted more stringent

restrictions regarding the interception of wire and electronic communications.[52] Among those states are California (*see* individual right of privacy in Cal. Const. Art. 1 §1) and New Jersey[53] (*see* the pendent statutory claims in the *Pietrylo case* discussed in note 46 supra and in Brownstone eWorkplace II, supra note 2, at 24-25 (.pdf pp. 29-30) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=24>).

Many states have passed or are currently considering legislation that would prohibit employers from asking employees for social media passwords,[54] and others have enacted more comprehensive privacy legislation.[55] 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."[56] *See also* the discussion at Section III(B)(3) below.

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.

---

[52] *See* Brownstone eWorkplace II, supra note 2, at 26 (.pdf p. 31) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=31>.

[53] *See , e.g., Ehling v. Monmouth-Ocean Hospital Service Corp.,* Civ. No. 2:11-CV 033305 (WJM) (D.N.J. May 30, 2012) (dismissing claim under state analogue to Wiretap Act; but denying motion to dismiss common-law invasion claim) <docs.justia.com/cases/federal/district-courts/new-jersey/njdce/2:2011cv03305/260497/23/0.pdf?1338465179>.

[54] *See, e.g.,* Md. Ann. Code § 3-712 <http://shorl.com/grofatujysija> and Illinois <ilga.gov/legislation/publicacts/fulltext.asp?Name=097-0875>, both already signed into law. *See also* Section VB)(3) below, mentioning those new laws as well as now-effective similar ones in Michigan and California. *See also* Del. House Bill No. 108 <legis.delaware.gov/LIS/lis146.nsf/vwLegislation/HB+308/$file/legis.html>.

[55] 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>.

[56] *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").[57] Such a cause of action confers federal subject matter jurisdiction, enabling the suit to proceed in federal court.

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 version of this sub-section,[58] 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.

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.[59] 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."

The category of potential plaintiffs includes not only the owner of an improperly accessed computer but also third parties who "have rights to data stored on" that computer. As to potential defendants, the category of "violator" under Section 1030(g) may include not only a complete stranger but also authorized users, such as: a university student who goes beyond his/her access rights; and/or an employer rendered vicariously liable for an employee's actions.

Employers face two hurdles in establishing their CFAA claims: alleging the requisite

---

[57] *Id.* at 27-32 (.pdf pp. 32-37).

[58] Brownstone eWorkplace II, supra note 2, at 27-30 (.pdf pp. 32-35) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=31>.

[59] The Computer Fraud & Abuse Act ("CFAA") prohibits: "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); and "knowingly caus[ing] the transmission of a program, information, code, or command . . . [that] intentionally causes damage without authorization to a protected computer," 18 U.S.C. § 1030(a)(5)(A)(i)). *See generally* Brownstone, Robert D., 9 *Data Security & Privacy Law,* Privacy Litig. Ch. §§ 9:3 through 9:16 (West 2010 & Supp. 2012).

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

As indicated by an April 10, 2012 Ninth Circuit decision,[60] 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. In the past few years alone, there have been several Circuit court opinions and dozens of U.S. district court decisions in this area. The outcomes in those decisions have split roughly evenly. A list of citations – accompanied by links and parenthetical summaries – for most of those cases is available on request from the author of this white paper.

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. In response to a motion to dismiss attacking the sufficiency of the authorization element, Plaintiffs have routinely counter-argued that: "authorized access" extended only to performance of job duties; and, insofar as the employee downloaded information for nefarious purposes, the access became unauthorized. The case-law on this "authorized access" sub-issue has split throughout this decade. The last couple years, though, have, on the whole, seen a pro-employee tilt. Significantly, in September 2009, the Ninth Circuit became only the second circuit court to weigh in, in *LVRC Holdings LLC v. Brekka*.[61] Given that *Brekka* created an *appellate* court split – between the Seventh and Ninth Circuits – some commentators have been predicting that the U.S. Supreme Court may grant certiorari to resolve this issue.[62]

The *Brekka* court held that an employee with authorization to access company information did not violate the CFAA by copying many files and e-mailing them to his personal email account prior to resigning. The parties did not have a written employment agreement; and the employer did not maintain guidelines prohibiting employees from emailing work documents to non-work computers. The CFAA claim failed because the "without authorization" element exists only when an employee has not received permission to use a computer/system for any purpose or when the owner of the computer has rescinded previously granted permission.[63] The court thus affirmed the former employee's

---

[60] *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>.

[61] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-35 (9th Cir. 2009) <ca9.uscourts.gov/datastore/opinions/2009/09/15/07-17116.pdf>. *See also* Fenwick & West LLP, *Employee With Authorization to Access Company Documents Did Not Violate Any Law by Copying Files Before Resigning*, Emp. Brief (Oct. 15, 2009) <fenwick.com/publications/6.5.4.asp?mid=51&WT.mc_id=EB_101509#employee>.

[62] *See, e.g.,* Nick Akerman, *Will the justices rule on the Computer Fraud and Abuse Act?* Nat'l L. J. (Sep. 23, 2009) <www.dorsey.com/files/upload/akerman_computer_fraud_july09.pdf>. *But see* Amy E. Bivens, *Brekka Case Shows Need for Comprehensive Strategy to Shield Data From Insider Misuse*, Electronic Commerce & Law Report (ECLR) (BNA Sep. 30, 2009) <http://www.tradesecretslaw.com/uploads/file/Sieve.pdf>.

[63] 581 F.3d at 1135.

motion for summary judgment on the CFAA claim against him.

In 2010, a number of federal district courts followed *Brekka*.[64] On the other hand, in 2010 and 2011, respectively, two circuit courts – the Fifth and Eleventh chose *not* to follow *Brekka* when hearing appeals regarding CFAA criminal prosecutions.[65]

Similarly, in 2010 and 2011, a number of federal district courts followed *Citrin*'s broad view.[66] But, then, in 2012 the Ninth Circuit rejoined the anti-*Citrin* camp in *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>. In that criminal case, in the course of affirming the dismissal of a five-count indictment, the appellate court adopted the pro-employee view. As summarized by some of this White Paper's author's colleagues:

> in a[ ] decision penned by Judge Kozinski, [the Ninth Circuit] held that an employee could not be criminally liable under the . . . "CFAA" . . . for "exceeding authorized access" to an employer's computer by accessing proprietary information in violation of the employer's written policies. In so holding, the Ninth Circuit reversed course from the initial panel decision, and entrenched its split from other circuits that have interpreted the CFAA's "exceeds authorized access" prong to cover violations of an employer's clearly disclosed computer use policy. The *Nosal* decision clarifies the Ninth Circuit's view that the CFAA targets true "hacking," and not violations of company computer use policies or website terms of service.

Fenwick & West LLP, *En Banc Ninth Circuit Limits Scope of Computer Fraud and Abuse Act; Terms of Use Do Not Restrict "Authorized Access",* Litigation

---

[64] *See, e.g., Consulting Prof'l Resources v. Concise Technologies LLC,* 2010 WL 1337723 (W.D. Pa. Mar. 9, 2010) <ecf.pawd.uscourts.gov/doc1/15712169362>; *Bell Aero. Servs. v. U.S. Aero Servs.*, 690 F. Supp. 2d 1267, 1272-73 (M.D. Ala. Mar. 5, 2010) (rejecting the Seventh Circuit's broad interpretation of the CFAA in *Citrin* and following the Ninth Circuit's approach in *Brekka*) <pub.bna.com/eclr/09cv141_030510.pdf>; *Clarity Servs., Inc. v. Barney*, 698 F. Supp.2d 1309 (M.D. Fla. Feb. 26, 2010) (granting summary judgment to Defendant/ex-employee; "[t]o show that [ex-employee] exceeded his authorized access to the laptop or accessed the laptop without authorization, [Plaintiff/ex-employer] must evidence an attempt to restrict [Defendant]'s access to the laptop[;]. . . . [f]urthermore, [Plaintiff] failed to impose any restriction on [Defendant]'s access to the laptop after he resigned") <https://ecf.flmd.uscourts.gov/doc1/04717880542>.

[65] *United States v. John*, 597 F.3d 263, 273 (5th Cir. Feb. 9, 2010) (in criminal prosecution, " [*Brekka*'s] reasoning at least implies that when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access'") <http://www.ca5.uscourts.gov/opinions%5Cpub%5C08/08-10459-CR0.wpd.pdf>; *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. Dec. 27, 2010) (distinguishing *Brekka*) <http://www.ca11.uscourts.gov/opinions/ops/200915265.pdf>.

[66] *See* decisions cited in Brownstone eWorkplace II, supra note 2, at 29 (.pdf p. 34) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=34>.

Alert (Apr.11, 2012) <http://www.fenwick.com/publications/Pages/En-Banc-Ninth-Circuit-Limits-Scope-of-Computer-Fraud-and-Abuse-Act.aspx>.[67]

Even more recently, the Fourth Circuit followed the *Nosal* view in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. July 26, 2012) ("[o]ur conclusion here likely will disappoint employers hoping for a means to rein in rogue employees[; b]ut we are unwilling to . . . transform[] a statute meant to target hackers into a vehicle for imputing liability to workers who . . . disregard a use policy") <http://www.ca4.uscourts.gov/Opinions/Published/111201.P.pdf>.

Some commentators, including Fenwick & West's Sebastian Kaplan, interpret some of the CFAA case law as comprising a third approach that focuses on the parties' specific agreements or employer policies. While *Citrin* and *Brekka* analyzed the meaning of "without authorization," courts adopting the contract view rely on the meaning of "exceeds authorized access." Under the contract view, an employee exceeds authorized access if he or she accesses information and uses it for purposes that are explicitly prohibited by the employer or computer owner. Followers of this view include not only the *John* and *Rodriguez* decisions cited in footnote 65 above but also a number of district courts that issued decisions in 2011.[68]

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.[69]

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

---

[67] For perspectives of other commentators, *see also* Harvey Silverglate, *Careful What You Click: The CFAA, The Ninth Circuit, And Your Right to Read This Blog,* Forbes (Apr. 13, 2012) <http://www.forbes.com/sites/harveysilverglate/2012/04/13/careful-what-you-click-the-cfaa-the-ninth-circuit-and-your-right-to-read-this-blog/print/>; Ginny LaRoe, *With 9-2 Ruling, Circuit Narrows Scope of Computer Fraud and Abuse Act*, Recorder (Apr. 10, 2012) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202548590609>; Ginny LaRoe, *Computer Fraud Opinion is Classic Kozinski*, Legalpad (Apr. 10, 2012) <legalpad.typepad.com/my_weblog/2012/04/computer-fraud-opinion-is-classic-kozinski.html>.

[68] *Id.* at 30 (.pdf p. 35) @ n. 123 and accompanying text.

[69] *Id.* at 30-31 (.pdf pp. 35-36).

completeness or usability of data or information on a computer system."[70]

d. Other CFAA Hot Topics

Some other CFAA issues warrant mentioning. First, in early 2011, a Florida federal court rejected a seemingly frivolous CFAA counterclaim against a former employee, where the allegations essentially only encompassed Plaintiff's excessively surfing her own Facebook page and personal webmail account – rather than improperly accessing any employer data. *Lee v. PMSI, Inc.*, 2011 WL 1742028 (M.D. Fla. May 6, 2011) <http://www.noncompetenews.com/file.axd?file=2011/5/Lee%20v.%20PMSI.pdf>.

Then, on another CFAA front, in 2011 an employer survived a motion to dismiss in a case where, after a home building company allegedly terminated eight employees for pro-union activity, the employees' union encouraged its supporters to inundate the e-mail and phone systems of the employer's sales offices and executives with thousands of messages in support of the discharged workers. *Pulte Homes, Inc. v. LIUNA* 648 F.3d 295 (6th Cir. Aug. 2, 2011) <ca6.uscourts.gov/opinions.pdf/11a0200p-06.pdf>. The communications overloaded both the e-mail and voicemail systems, and prevented customers from reaching the company and employees from accessing messages. The employer sued the union, alleging several state tort claims and CFAA violations and moved to enjoin the union's e-mail and phone campaign. After the trial court dismissed the suit, the employer appealed as to the CFAA claims. The Sixth Circuit reversed, holding that the company adequately stated a "transmission" claim under the CFAA, *i.e.*, that the union "knowingly cause[d] the transmission of a program, information, code or command, and as a result of such conduct, intentionally cause[d] damage without authorization, to a protected computer." *Id.* at 301. The court found that the two key elements of the claim, damages and intent, were satisfied: the diminished ability to send and receive calls and e-mails was sufficient damage to the company, and the company alleged that the union had the "conscious purpose" of causing damage to the company's computer system. *Id.* at 303. The Court remanded for a jury trial.

To learn more about *Pulte*, *see Bombardment Of Employer's Email And Phone Systems States A Claim For Violation Of Computer Fraud And Abuse Act*, Fenwick Emp. Brief (Sep. 19, 2011) <fenwick.com/publications/6.5.4.asp?mid=76&WT.mc_id=EB_091911#bombardment>, on which the preceding discussion is largely based. Note that it is unclear whether the *Pulte* appellate court's theory will take hold, especially in light of seemingly contrary case-law on the issue of trespass to electronic information systems.

Another developing area of law under the CFAA involves ownership of social media accounts that employees use for both professional and personal purposes. Last year, a federal district court judge rejected an employee's argument that her employer violated the CFAA when it took control of her LinkedIn account after firing her. According to the court, the employee's claims that she had lost business opportunities as a result of her ex-employer's

[70] *Id.* at 31-32 (.pdf pp. 36-37).

access were "simply not compensable under the CFAA."[71]

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.[72] In the past several years, the NLRB and the courts have begun to dig in and wrestle with the parameters of protection of concerted activity in the 21st Century context.

Late 2010 ushered in a new era of scrutiny, when an NLRB Complaint in the social-media context resulted in a settlement. Though it did not proceed to adjudication, that case nonetheless became a cautionary tale as to discriminatory enforcement of a TAUP. "A complaint issued by the NLRB's Hartford regional office on October 27[, 2010] allege[d] that an ambulance service illegally terminated an employee who had posted negative remarks about her supervisor on her personal Facebook page."[73] "The complaint also allege[d] that the company, American Medical Response of Connecticut, Inc. [AMR], . . . maintained and enforced an overly broad blogging and internet posting policy."[74] After much publicity and speculation in the mainstream media and in the legal press,[75] the

---

[71] *Eagle v. Morgan*, 2012 WL 4739436 (E.D. Pa. Oct. 4, 2012) <digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1153&context=historical&sei-redir=1>. *See* Megan Leonhardt, *Separating Mobile Work And Play Helps Curb Discovery Issues*, Law360 (Oct. 23, 2012) <http://www.law360.com/legalindustry/articles/389017/separating-mobile-work-and-play-helps-curb-discovery-issues>; Julia E. Judish, Thomas N. Makris, and Amy L. Pierce, *Drawing the Line Online: Employers' Rights to Employees' Social Media Accounts*, S.F.D.J. (Oct. 22, 2002) <http://www.pillsburylaw.com/siteFiles/Publications/AlertOctober2012Litigation_DrawingtheLineOnline_EmployersRightstoEmployeesSocialMediaAccounts.pdf>; Deanne Katz, *Employers Can Hijack Your LinkedIn Account, Court Rules*, Findlaw Technologist (Oct. 17, 2012) <blogs.findlaw.com/technologist/2012/10/employers-can-hijack-your-linkedin-account-court-rules.html >; Timothy B. Lee, *Judge: Takeover of Employee LinkedIn Account Doesn't Violate Hacking Law*, ArsTechnica (Oct. 8, 2012) <arstechnica.com/tech-policy/2012/10/court-taking-over-employees-social-media-account-a-ok-under-cfaa/>; Eric Goldman, *Battle Over LinkedIn Account Between Employer and Employee Largely Gutted--Eagle v. Morgan*, Technology & Marketing Law Blog (Oct. 7, 2012) <blog.ericgoldman.org/archives/2012/10/court_dismisses_8.htm>.

[72] 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#page=37>.

[73] News Release, *Complaint alleges Connecticut company illegally fired employee over Facebook comments,* NLRB Office of the General Counsel (Nov. 2, 2010) <http://mynlrb.nlrb.gov/link/document.aspx/09031d45803c4e5e>.

[74] *Id.*

[75] *See, e.g.,* Eli M. Kantor and Zachary M. Cantor, *Your Social Media Policy Needs a Status Update*, Daily J. (Nov. 26, 2010); Michael A. Sands and Dan Ko Obuhanych, *Will a 75-Year-Old Labor Relations law Help Shape the Future of Social Media Regulation*, Daily J. (Nov. 17, 2010) (available on request from this White Paper's author's colleagues); Brian Elzweig and Donna K. Peeples , *When Are Facebook Updates a Firing Offense?* Harv. Bus. Rev. (Nov. 10, 2010) <http://blogs.hbr.org/cs/2010/11/when_are_facebook_updates_a_fi.html>.

matter settled on February 7, 2011.[76] As characterized by the NLRB, "[u]nder the terms of the settlement . . ., the company agreed to revise its overly-broad rules to ensure that they do not improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others while not at work, and that they would not discipline or discharge employees for engaging in such discussions."[77]

Since the *AMR* settlement, there has been a flurry of additional NLRB activity in the social-media context. *See* Section V(B)(3) for a discussion of some of those recent developments and proceedings tackling whether employee posts constitute employment terms and/or conditions. Regardless of the gist of this activity's anticipated progeny (i.e., ultimately one or more Circuit court decisions), many employers regularly permit limited personal use of their e-mail systems and may solicit input from their employees on those systems. Employers therefore 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.

Moreover, at least for now – while it is unclear which overall standard will take hold long-term – employers may want to avoid splitting hairs in the pertinent provisions of their policies. They may thus want to avoid the "organization"-type prohibitions altogether. 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.

5. Countervailing Concern # 2 – Avoiding Invasion of Privacy Claims[78]

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.[79] Most decisions regarding the interception of a private employee's e-mail continue to find

---

[76] Settlement Agreement, *American Medical Response of Connecticut*, No. 34-CA-12576 (Feb. 7, 2011) <minnesotaemploymentlawreport.com/NLRB%20Facebook%20Settlement.pdf>. *See also* Leigh Kamping-Carder, *Landmark NLRB Facebook Case Ends With Settlement*, Law360 (Feb. 7, 2011) <law360.com/print_article/224315?section=topnews>; Stephanie Armour, *American Medical Settles Case in Facebook Dismissal*, Bloomberg (Feb. 7, 2011) <bloomberg.com/news/print/2011-02-07/american-medical-settles-u-s-case-in-dismissal-tied-to-facebook.html>.

[77] News Release, *Settlement reached in case involving discharge for Facebook comments,* NLRB Office of Pub. affairs (Feb. 8, 2011) <http://www.nlrb.gov/news/settlement-reached-case-involving-discharge-facebook-comments>.

[78] *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.pdf#page=40>.

[79] *See* SAMPLES linked from Appendix A of Brownstone eWorkplace II, supra note 2 (.pdf p. 67).

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.[80] 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.[81] *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/FACTA and State-Analogues[82]

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 focus of this sub-section. It is worth noting first, though, that, in August 2010, Massachusetts, in SB 2583,[83] enacted some restrictions on the latter type of background check, at least in initial written applications. Some of the provisions of SB 2583 – a/k/a the CRIMINAL OFFENDER RECORD INFORMATION (CORI) Act –took effect in November 2010; and some others took effect in February 2012.

Moreover, 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) <http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm>. The highlights are discussed by some colleagues of the author of this White Paper in Fenwick & West, *EEOC Provides Guidance Regarding Use Of Criminal History In Employment Decisions,* Employment Brief (May 11, 2012)

---

[80] 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).

[81] *See, e.g.*, SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 1, § III(B)-(D), at App. D-3 to D-4; SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 2, §§ I, at App. D-7, II, at D-8; SAMPLE ELECTRONIC MAIL POLICY, § II, at App. D-11, all available at <http://fenwick.com/fenwickdocuments/eworkplace_policies_materials_public_sector_eeo_8-28-09.pdf#page=142>.

[82] For more detail on this topic, *see* Brownstone eWorkplace II, supra note 2, at 36-38 (.pdf pp. 41-43) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=41>.

[83] 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>.

<www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-May-2012.aspx?WT.mc_id=EB_051112#eeoc>.[84]

Note, though, that a 2012 federal court decision found that, in an enforcement lawsuit, the EEOC can be subjected to a 30(b)(6) deposition by an employer accused of racially (and gender-based) discriminatory criminal background. *EEOC v. Freeman*, 2012 WL 3536752, 115 Fair Empl.Prac.Cas. (BNA) 1488 (D. Md. Aug. 14, 2012) <gpo.gov/fdsys/pkg/USCOURTS-mdd-8_09-cv-02573/pdf/USCOURTS-mdd-8_09-cv-02573-3.pdf>. *But see EEOC v. Freeman*, 2012 WL 6649195 (D. Md. Dec. 19, 2012) (denying motion to compel broader scope of deposition) <gpo.gov/fdsys/pkg/USCOURTS-mdd-8_09-cv-02573/pdf/USCOURTS-mdd-8_09-cv-02573-4.pdf>.

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").[85] The FCRA applies to private and public entities alike.

In addition, bear in mind that many states have analogous statutory schemes that are ostensibly stricter than the EEOC guidelines and/or than the FCRA.[86] For example, in recent years, in light of high unemployment rates, several states have gone even farther, generally banning employment decisions from being based on credit history, with exceptions for certain types of employers and/or positions.[87] There are now eight states in this category.[88] For example, on October 9, 2011, California Governor Jerry Brown signed into law AB 22, effective January 1, 2012. <leginfo.ca.gov/pub/11-12/bill/asm/ab_0001-0050/ab_22_bill_20111009_chaptered.pdf>. Moreover, Congress

---

[84] *See also* Paul Salvatore, *Digging Deeper into Criminal Checks*, HRE Online (July 17, 2012) <http://www.hreonline.com/HRE/view/story.jhtml?id=533349293>; Joseph McCafferty, *EEOC Issues New Guidance on the Use of Criminal Records*, Compliance Week (Apr. 26, 2012) <http://www.complianceweek.com/eeoc-issues-new-guidance-on-the-use-of-criminal-records/printarticle/238435/> (subscription may be required).

[85] *See generally FTC Testifies on the Rights of Employees Under the Fair Credit Reporting Act* (10/20/10) <www.ftc.gov/opa/2010/10/faircredit.shtmwww.ftc.gov/opa/2010/10/faircredit.shtm> (linking to <http://www.ftc.gov/os/testimony/101020eeoctestimony.pdf>).

[86] For a compilation and overview, *see* Lester Rosen, *State Law and Other Compliance Issues*, at 35-44, Employment Screening Resources (ESR) (Aug. 1, 2012) <http://media.straffordpub.com/products/pre-employment-background-screening-after-eeocs-new-guidance-2012-08-01/presentation.pdf#page=35>.

[87] Brownstone eWorkplace II, supra note 2, at 37-38 (.pdf pp. 42-43) @ nn. 155-157 and accompanying text (California, Oregon and Washington join Hawaii) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=41>.

[88] Rosen, supra note 86, at 44.

considered, but did not enact, a similar ban, with similar exceptions for when these types of background checks would be permissible.[89]

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 emerging principles in this area seem to be as follows:[90]

- 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 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 regarding existing employees, an applicant's posted content demonstrates a lack of ability to do, or interest in, the job, presumably there is no problem with the prospective employer relying 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?

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. 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.[91]

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. The FTC has sent mixed signals as to the defensibility of that approach. In one instance, the FTC approved the potential legality of a start-up company, "Social Intelligence," <http://www.socialintelligencehr.com/>, which performs social-media background

---

[89] H.R. 3149 <http://thomas.loc.gov/cgi-bin/bdquery/z?d111:h.r.03149:> (latest action Sep. 23, 2010).

[90] Brownstone eWorkplace II, supra note 2, at 38-41 (.pdf pp. 43-46) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=43>.

[91] *Id.*

checks on applicants.[92] More recently, though, the FTC issued warning letters to purveyors of mobile apps that purport to enable online background checks.[93]

As reflected in Slide 31 of Appendix E, 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. Indeed, websites, social media pages and associated apps intent to solicit, collect and gather such personal data.[94]

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. 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. *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>.

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 would seem to overreach, especially in the public sector context.[95]

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

---

[92] *Id.* at 39 (.pdf p. 44), at footnotes 165-66.

[93] *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#ftc>.

[94] *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>.

[95] *See* Abigail Rubinstein, 5 Questions Employers Shouldn't Ask Job Applicants, law360 (Nov. 30, 2012) <http://www.law360.com/employment/articles/397482>; Debbie Kaminer, *Can Employers Ask Applicants for Social Media Login Information?*, N.Y.L.J. (July 27, 2012) <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1342981750935>; Philip Gordon, *Is it Really Illegal to Require an Applicant to Disclose her Password to a "Friends-Only" Facebook Page?* Workplace Privacy Counsel (March 8, 2011) <privacyblog.littler.com/2011/03/articles/social-networking-1/is-it-really-illegal-to-require-an-applicant-or-employee-to-disclose-her-password-to-a-friendsonly-facebook-page/> (raising argument that, as in Maryland public sector situation, applicant's consent could arguably distinguish the *Pietrylo*-type situation discussed in Section II(A)(1)(c) above).

received a tremendous amount of press coverage, including as to Facebook's vehement objections.[96]

Moreover, on April 1, 2012, the Maryland legislature became the first state to pass legislation banning employers from asking current or former employees to disclose a user name or passwords for a personal online account.[97] On May 2, 2012, the Maryland Governor quickly signed the bill into law, effective October 1, 2012. On May 22, 2012, Illinois followed suit, with its own bill, signed by the Governor August 1, 2012 and effective January 1, 2013 <ilga.gov/legislation/publicacts/fulltext.asp?Name=097-0875&print=true&write>. Similar laws went into effect in Michigan on December 28, 2012 <www.legislature.mi.gov/documents/2011-2012/billenrolled/House/htm/2012-HNB-5523.htm> and California on January 1, 2013 <http://www.leginfo.ca.gov/pub/11-12/bill/asm/ab_1801-1850/ab_1844_bill_20120927_chaptered.pdf>. Other states, including Delaware, Massachusetts, Minnesota, New Jersey, and Washington, have introduced bills that would prohibit employers from asking employees or job applicants for their social media login information.[98] Note also that federal legislation in this area is possible.[99]

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) and then to dispose of it securely when the information is no longer needed including per the FTC's Disposal Rule under FACTA). A stark example involved NASA, which fought for years to

---

[96] Brian Donohue, *Applicants Coerced Into Surfing Facebook While Employers Watch*, threatpost (Mar. 12, 2012) <threatpost.com/en_us/blogs/applicants-coerced-surfing-facebook-while-employers-watch-031212>; 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/>; Kayla Webley, *Background Check for the Digital Age: Employers, Colleges Insist on Full Facebook Access*, Time (Mar. 6, 2012) <moneyland.time.com/2012/03/06/background-check-for-the-digital-age-employers-colleges-ask-for-facebook-passwords/>.

[97] Md. SB 433 is now Md. Ann. Code § 3-712 <http://shorl.com/grofatujysija>

[98] *See also* Section II(B)(2) above; Behnam Dayanim, *Employee Privacy Forces Legislation*, Recorder (Aug. 8, 2012) ("these 'bullet bills,' by imposing a bright-line rule narrowly focused on the latest controversy, represent a missed opportunity both to update the SCA to reflect today's technology and to re-engage the debate over the broader policy questions the new digital world creates.") <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202566686683>; Debbie Kaminer, *Can Employers Ask Applicants for Social Media Login Information?*, N.Y.L.J. (July 27, 2012) <www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1342981750935>.

[99] Social Networking Online Protection Act (SNOPA), H.R. 5050 (Apr. 27, 2012) <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.5050:>, which was reintroduced Feb. 6, 2013. *See also* Thomas I. Barnett, *Privacy Laws Cause Discovery Woes*, Recorder (June 20, 2012) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202560186389>; Allen Smith, *Potentially Illegal Practice of Demanding Passwords Criticized*, SHRM (April 3, 2012) <http://www.shrm.org/LegalIssues/FederalResources/Pages/DemandingPasswords.aspx>; Kashmir Hill, *Senator Wants To Make It Illegal For Employers To Ask For Your Facebook Password*, Forbes (Mar. 22, 2012) <http://www.forbes.com/sites/kashmirhill/2012/03/22/senator-wants-to-make-it-illegal-for-employers-to-ask-for-your-facebook-password/>; Catherine Ho, *Md. employers cannot collect Facebook passwords*, Wash. Post (Apr. 15, 2012) <http://www.washingtonpost.com/business/capitalbusiness/md-employers-cannot-collec/t-facebook-passwords/2012/04/13/gIQAZwQtJT_story.html>.

defend its right to seek illegal drug-use information on applicants for employment by NASA federal contractors. See *Nelson v. NASA*, 1131 S. Ct. 746 (Jan. 19, 2011) <http://www.supremecourt.gov/opinions/10pdf/09-530.pdf>, as discussed at Brownstone eWorkplace II, supra note 2, at 40-41 (.pdf pp. 45-46) @ notes 170-77 and accompanying text. <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=45>.

Ironically, though, as discussed in footnote 14 above, not long thereafter, a couple unencrypted NASA laptops were stolen, leading to the exposure of lots of private information, some of which had been gathered in the very background checks at issue in the *Nelson* case.

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 may sometimes intrude into an employee's reasonable expectation of privacy. *See generally* Brownstone eWorkplace II, supra note 2, at 41-42 (.pdf pp. 46-47) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=46>.[100]

[100] On the issue of smartphone seizure under the search-incident-to-arrest exception to the Fourth Amendment's protections, *see also Commonwealth v. Phifer*, 463 Mass. 790, 979 N.E.2d 210, 216 (Dec. 5, 2012) ("limited search of the defendant's cellular telephone to examine the recent call list was a permissible search incident to the defendant's lawful arrest") <http://caselaw.findlaw.com/ma-supreme-judicial-court/1617338.html>; *Commonwealth v. Berry*, 463 Mass. 800, 979 N.E.2d 218, 223 (Dec. 5, 2012) (same; "police . . . conducted a very limited search of the cellular telephone, pressing one button to view the recent call list, reading the most recent telephone number displayed, and calling it") <http://epic.org/privacy/location_privacy/Commonwealth-v-Berry.pdf>; Cal. S.B. 914 (legislation seeking to overturn *People v. Diaz,* 51 Cal. 4th 84, 244 P.3d 501 (2011) vetoed Oct. 9, 2011 by Gov. Brown; veto sustained Mar. 1, 2012) <http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_914&sess=CUR&house=B&author=leno>; Perry L. Segal, *e-Discovery California: The 'Leno' Show Seeks to Overturn Diaz: SB 914*, e-Discovery Insights (June 17, 2011) <http://www.ediscoverycalifornia.com/insights/2011/06/e-discovery-california-the-leno-show-seeks-to-overturn-diaz-sb-914.html>. *Compare People v. Rangel*, --- Cal.Rptr.3d ----, 2012 WL 2149779 (Cal. App. 1 Dist. June 14, 2012) (as to separate Fourth Amendment issue, upholding seizure of cellphone pursuant to search warrant issued as to defendant's home) <http://www.courts.ca.gov/opinions/documents/A132664.PDF>. Employers should be aware that an employee's smartphone could be seized by a policeman and/or readily forensically imaged, even on the spot. *See, e.g.,* Greg Buckles, *Mobile Discovery – Are You Ready For It? eDiscovery J.* (Apr. 9, 2012) <http://ediscoveryjournal.com/2012/04/mobile-discovery-are-you-ready-for-it/> (citing Matt Brian, *US Police Can Copy Your iPhone's Contents In Under Two Minutes*, TNW (Apr. 20, 2011) <http://thenextweb.com/us/2011/04/20/us-police-can-copy-your-iphones-contents-in-under-two-minutes/>); Moreover, only one reported decisions to reign in overzealous authorities that wish to obtain access to all cloud-stored information as to which a smartphone or a tablet (*e.g.*, and iPad) could provide access and login information. *See USA's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius,* 2011 WL 991405 (W.D. Wash. 2/11/11) <cdn.volokh.com/wp/wp-content/uploads/2011/03/CunniusSearchOpinion.pdf>.

2. Personal Searches[101]

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 that the search was justified 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.

B. Video Surveillance – *e.g.*, of Vehicle-Operators to Deter Smartphone-Use-While Driving[102]

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.[103] In any event, as a matter of overall common-sense/decency, employers should not set up video surveillance in restrooms, changing rooms, and other private areas within the workplace. Moreover, states such as California have statutes outright prohibiting videotaping in certain locations.

In late 2009 a rail labor union sued in federal and state court, seeking to enjoin a plan that the Complaint described as "install[ing] and operat[ing] recording cameras and related equipment to perform video and audio surveillance in locomotive cabs . . . [to] monitor and record every act of the locomotive engineers operating [Southern California] Metrolink trains."[104] Those tapings were intended to catch train engineers texting while driving. Ironically, the very next day, two Northwest Airline pilots lost their way and overshot an airport by 150 miles, allegedly because they were distracted by their use of their laptops.[105]

---

[101] *See generally* Brownstone eWorkplace II, supra note 2, at 42 (.pdf p. 47) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=47>.

[102] *See generally id.* at 43-45 (.pdf pp. 48-50).

[103] For a recent examination of facial recognition technologies and privacy concerns, including best practices for companies that use facial recognition technologies, *see* Federal Trade Commission, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (October 2012) <http://ftc.gov/os/2012/10/121022facialtechrpt.pdf>. European regulators are much stricter. *See, e.g.,* Somini Sengupta and Kevin J. O'Brien, *Facebook Can ID Faces, but Using Them Grows Tricky*, N.Y. Times (Sep. 21, 2012) <nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html>. *See also* Brownstone eWorkplace II, supra note 2, at 9 (.pdf p. 14), at footnotes 45-46 <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=14>.

[104] *See, e.g.,* Complaint, *Bhd. of Locomotive Eng'rs and Trainmen v. So. Cal. Reg'l Rail Auth.*, Case No. CV09-7601 PA (C.D. Cal. Oct. 20, 2009) <https://ecf.cacd.uscourts.gov/doc1/03109002572>, eDocket in related Case No. 09-cv-08286 <https://ecf.cacd.uscourts.gov/cgi-bin/DktRpt.pl?588578789685931-L_674_0-1>.

[105] Reuters, *Pilots on Wayward Jetliner Were Using Laptops: Officials* (Oct. 26, 2009) <reuters.com/article/idUSTRE59P4VB20091026>.

Subsequently, in the railroad case, the court granted Defendant's Motion for Judgment on the Pleadings <ecf.cacd.uscourts.gov/doc1/031110444467> dismissing all claims.

Over the past few years there have been a number of administrative agency efforts directed at prohibiting those who drive for a living from using cell phones while driving, except in cases of emergency.[106] As to drivers *and* other types of workers, employers should consider implementing a written policy that – just as with other forms of monitoring – provides employees with advance notice that they may be subject to video surveillance.[107]

C. GPS Tracking – including RFID and GPS

See generally Brownstone eWorkplace II, supra note 2, at 45-46 (.pdf pp. 50-51) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=50>. *See also* Bradford LeHew, 11 PVLR 921, BNA Privacy & Data Security Law Report (June 11, 2012) (applying to workplace policies the principles of Fourth Amendment case of *U.S. v. Jones*, 132 S.Ct. 945, 181 L.Ed.2d 911 (Jan. 23, 2012) <http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>)) <http://privacylaw.bna.com/pvrc/display/batch_print_dialog.adp?fedfid=26885526&vname=pvlrnotallissues&jd=a0d2g0k3c7&split=0> (subscription required). As to the implicit *ability* to monitor, *see* these discussions of various smartphones apps premised on sharing individuals' locations: Nick Bilton, *Girls Around Me: An App Takes Creepy to a New Level* , N.Y. Times (Mar. 30, 2012) <bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level>; Nicole Perlroth, A*fter Rapes Involving Children, Skout, A Flirting App, Bans Minors*, N.Y. Times (June 12, 2012) <bits.blogs.nytimes.com/2012/06/12/after-rapes-involving-children-skout-a-flirting-app-faces-crisis>.

D. "Off-Duty" Activities

As discussed in *id.* 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") <http://White-Paper-8-09-at-62.notlong.com>.

2. Substance Use

For this second area, *see* Brownstone eWorkplace II, supra note 2, at 47 (.pdf p. 52) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-

---

[106] Brownstone eWorkplace II, supra note 2, at 45 (.pdf p. 50) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=50>.

[107] *See generally id.* at 45 (.pdf p. 50) @ nn. 204-05 and accompanying text (noting, among other things, that video surveillance may be a mandatory bargaining subject in union shops).

Media_Materials_NELI_Brownstone_4-3-12.pdf#page=50>. *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) <http://www.tsc.state.tn.us/sites/default/files/paytonstevenopn.pdf>.

3. Dating and Intimate Relationships

For a relatively detailed discussion of this third area, *see id.* at 47-48 (.pdf pp. 52-53).

In recent years, key developments have often focused on police or school teachers as to whom a code of conduct applied.[108] Of course, when a case involves a teacher's alleged intimate relationship with a minor, many serious concerns are raised.[109] 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. In 2011, the Missouri legislature passed "the Amy Hestir Student Protection Act," (SB 54), <http://web.archive.org/web/20120425235704/http://www.colecountycourts.org/Missouri%20State%20Teachers%20vs%20Missouri.pdf>, namely a set of statutes seeking to restrict Internet contact between teachers and students of high school age and younger. The state's teachers sued to challenge the legality of the enactments on constitutional and other grounds.[110] A preliminary injunction promptly ensued <http://web.archive.org/web/20120425235704/http://www.colecountycourts.org/Missouri%20State%20Teachers%20vs%20Missouri.pdf>; but the case is still pending.[111]

This Spring, the New York City Department of Education (DOE) followed suit by issuing lengthy guidelines, providing in part that, other than in delineated exceptional circumstances, "employees should not communicate with students who are currently enrolled in DOE schools on personal social media sites." NYC DOE, *Social Media Guidelines* § E(1), at 4 & n.8 (April 30, 2012) ("[e]xamples of such communications

---

[108] *See, e.g., San Diego U.S.D. v. Comm'n on Prof'l Competence (Lampedusa)*, 124 Cal. Rptr. 3d 320 (Cal. App. 4 Dist. 5/3/11) (upholding firing for posting gay sex ad on Craig's-List) < http://caselaw.lp.findlaw.com/data2/californiastatecases/D057740.PDF>.

[109] Brownstone eWorkplace II, supra note 2, at 45-51 (.pdf pp. 50-56) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=50> @ ns. 220, 228, 232 and 234 and accompanying text, including *Spanierman v. Hughes*, 576 F. Supp. 2d 292 (D. Conn. 2008) (upholding contract non-renewal as to high school teacher, based on school superintendent's objections to nature of teacher's MySpace content and of associated communications with students) </www.ctemploymentlawblog.com/uploads/file/hughes.pdf>. *See also* Corey M. Dennis, *Legal Implications of Employee Social Media Use*, 93 Mass. L. Rev. No. 4, at 380,388-89 (.pdf pp. 8-9) (June 11, 2011) (discussing *Spanierman*) <massbar.org/media/1029395/legal%20implications%20.pdf>.

[110] *Missouri State Teachers Ass'n v. State of Missouri*, Petition for Injunctive Relief and Declaratory Relief, Case No. 11AC-CC00553 (Mo. Cir. Ct. Cole Cty. Aug. 19, 2011) <msta.org/news/Petition_final.pdf>; Kevin Murphy, *Missouri teachers sue to block social media law*, Reuters (Aug. 20, 2011) <reuters.com/article/2011/08/20/us-schools-missouri-suit-idUSTRE77J1QW20110820>; Eva Arevuo, *Missouri's "Facebook Law" is Misdirected* , Legally Easy (Aug. 9, 2011) <legallyeasy.rocketlawyer.com/missouris-facebook-law-is-misdirected-92955>.

[111] *Cf.* Ryan Tate, *Facebook Turns Schools Into Hellscapes of Abuse and Hysteria*, Gawker.com (Aug. 22, 2011) <gawker.com/5833288/facebook-turns-schools-into-hellscapes-of-abuse-and-hysteria>.

include, but are not limited to, 'friending,' 'following,' 'commenting, and posting messages") <http://schools.nyc.gov/NR/rdonlyres/BCF47CED-604B-4FDD-B752-DC2D81504478/0/DOESocialMediaGuidelines20120430.pdf#page=4>. *See also* AP, *NYC issues social-media guidelines for teachers*, First Amendment Center (5/2/12) (linking to various resources and articles) <http://www.firstamendmentcenter.org/nyc-issues-social-media-guidelines-for-teachers>.

4. Arrests and Convictions[112]

For a while, this 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.[113] 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. Some of the many scenarios that have come to the fore in the past few years are listed at Brownstone eWorkplace II, supra note 2, at 50-51 (.pdf p. 55-56) <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=55>.

In 2012, there were at least two decisions rejecting FMLA claims, each of which was premised on an employer's alleged improper reliance on one or more of an employee's Facebook posts. *See 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

---

[112] *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#page=50>.

[113] For some of the types of factual investigations possible by, among others, law enforcement, *see, e.g.,* Scott A. Freedman and Jessica A. Barajas, *Investigating Prospective Employees in the Information Age*, D.J. (Mar, 9, 2011) <mpplaw.com/files/Publication/46c2e1f7-bcf4-419a-9367-d017c8767cd2/Presentation/PublicationAttachment/f4112d0f-98be-4dde-8aaf-d4b899b76766/Investigating-Prospective-Employees.pdf>; Ken Strutin, *Criminal Law Resources: Social Networking Online and Criminal Justice*, LLRX (Feb. 28, 2009) <llrx.com/node/2150/print>. *See also* Joseph Goldstein, *In Social Media Postings, a Trove for Investigators*, N.Y. Times (Mar. 2, 2011) <http://www.nytimes.com/2011/03/03/nyregion/03facebook.html>.

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) <www.gpo.gov/fdsys/pkg/USCOURTS-ohnd-5_11-cv-00399/pdf/USCOURTS-ohnd-5_11-cv-00399-1.pdf>.

A very 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.[114] Some lawsuits have addressed whether such publicly displayed items can constitute trade secrets[115] and the related question of whether the widespread web availability of contact information can preclude organizations' internal contacts databases from being protectable as trade secrets.[116]

[114] Bruce Carton, *Who Owns a Terminated Employee's Twitter Account?* Legal Blog Watch (Oct. 4, 2010) (CNN's Rick Sanchez) <http://legalblogwatch.typepad.com/legal_blog_watch/2010/10/who-owns-a-terminated-employees-twitter-account.html>. For some policy-drafting tips – some of which are helpful and some of which seem extremely unrealistic for an employer that wants its employees to use their own social-media pages to hype the company – *see* Eric Syverson, *As rolodexes go online ownership is muddy*, L.A. & S.F. Daily J. (Feb. 3, 2012), available to Daily Journal subscribers via search at <http://tinyurl.com/DJ-Search> (citing *PhoneDog v. Kravitz*, No. C 11-03474 (N.D. Cal. 2012) (all company's Twitter passwords allegedly "confidential information"), eDocket available at <http://dockets.justia.com/docket/california/candce/3:2011cv03474/243145/>). *See also* Adam S. Walker, *Yours, Mine, or Ours? The Battle Over Social Media Content*, Wash. Lawyer (Aug. 2012) <dcbar.org/for_lawyers/resources/publications/washington_lawyer/august_2012/social_media.cfm> (also discussing *PhoneDog v. Kravitz*).

[115] *See, e.g.*, *Eagle v. Morgan,* 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011) (dismissing trade secrets counterclaim) <www.gpo.gov/fdsys/pkg/USCOURTS-paed-2_11-cv-04303/pdf/USCOURTS-paed-2_11-cv-04303-0.pdf>, discussed in Nick Akerman, *Company Computer Policies Risk Becoming Obsolete*, Nat'l L. J. (Apr. 10, 2012) <www.dorsey.com/files/upload/akerman_nlj_040212.pdf>.

[116] Brian Sumers, *As rolodexes go online ownership is muddy*, L.A. & S.F. Daily J. (Nov. 19, 2010), available to Daily Journal subscribers via search at <http://tinyurl.com/DJ-Search> (citing *Sasqua Group, Inc. v. Courtney*, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010) (availability of LinkedIn) <http://www.scribd.com/doc/38079477/Sasqua-Group-v-Courtney-E-D-N-Y-Aug-2-2010>, *as adopted by* 2010 WL 3702468 (Sep. 9, 2010) <http://docs.justia.com/cases/federal/district-courts/new-york/nyedce/2:2010cv00528/300764/16/0.pdf?1284024095>; *TEKSystems Inc. v. Hammernick*, Complaint, No. 10-00819 (Mar. 6, 2010) (use of LinkedIn to contact people) <http://www.ilr.cornell.edu/law/events/upload/TEKsystems-v-Hammernick.pdf>) . *Compare* the decision in the non-social-media-context *Pyro Spectaculars, Inc. v. Souza*, 2012 WL 968084 (E.D. Cal. Mar. 21. 2012) <http://docs.justia.com/cases/federal/district-courts/california/caedce/2:2012cv00299/234705/101/0.pdf?ts=1332405774>, discussed in James McNairy, *Fireworks Fly, California District Court Enjoins Former Pyrotechnics Company Employee From Soliciting Former Employer's Customers*, Seyfarth Shaw's *Trading Secrets* (Mar. 30, 2012) <tradesecretslaw.com/2012/03/articles/restrictive-covenants/fireworks-fly-california-district-court-enjoins-former-pyrotechnics-company-employee-from-soliciting-former-employers-customers/print.html>.

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.[117] 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.

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."[118] As discussed in Brownstone eWorkplace II, supra note 2, at 52-53 (.pdf pp. 57-58) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=57>, 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

---

[117] Dunn, Darrell, *Email is Exhibit A*, Info. Week (May 8, 2006) (quoting ePolicy Institute's Nancy Flynn) <http://www.informationweek.com/shared/printableArticle.jhtml;jsessionid=JVK0JEBYYBRZWQSNDLRSKH0CJUNN2JVN?articleID=187200562&_requestid=12387>.

[118] *See, e.g.*, SAMPLES linked off of Appendix A.

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) <www1.legis.ga.gov/legis/2003_04/gacode/16-9-93.html>.

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, supra note 2, at 53 (.pdf pp. 58) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=58>. 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[119]

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. Moreover, as soon as there is concern that a particular employee may bring a claim, an employer should consider obtaining a forensically sound image of each computer and laptop provided to that employee. Similarly, where misappropriation of trade secrets is suspected, prompt confiscation of computers, if possible, is a sound proactive approach.

[119] *See* Brownstone eWorkplace II, supra note 2, at 53-54 (.pdf pp. 58-59) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=58>.

c. International Caveat[120]

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.[121] 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/PDA's[122]

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, PDA's, and other company-issued mobile devices. In addition to laptops, 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.

---

[120] *See* Robert D. Brownstone, *Cross-Border eDiscovery* (Oct. 24, 2012) (lengthy slide deck) <http://content.westlegaledcenter.com/c1/programMaterial/WLEC/CrossBorderSlidesBrownstone10-24-12.pdf>; *see also* related video of "eDiscovery 3.0" panel, Blackstone Discovery (Oct. 24, 2012) at <http://www.blackstonediscovery.com/videos/#2> .

[121] *See* "adopted" revisions at "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century," at pp. 40-98 [.pdf pp. 41 – 99] (Jan. 25, 2012) (sandwiched between two lengthy explanations) <ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf#page=41>. For more resources, contact the author of this White Paper.

[122] 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#page=58>.

3. NLRB Pronouncements as to Prohibitions/Restrictions on Blogging, Posting, Social-Networking and Tweeting[123]

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.[124]

The *Pietrylo* decision discussed above highlights the challenges employers face with respect to employees' blogs and social networking sites that contain work-related speech.[125] 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.[126] The particular wording of `employers' social media policies is important, so employers should take the time to draft social media policies that will withstand NLRB scrutiny.[127]

---

[123] To learn more, *see* Brownstone eWorkplace II, supra note 2, at 55-60 (.pdf pp. 60-65) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=60>.

[124] *Id.*

[125] *See* Fenwick & West, *Jury Finds Employer Accessed "Private" MySpace.com Group Page In Violation Of The Federal Stored Communications Act*, Emp. Brief (Sep. 9, 2009) <http://www.fenwick.com/docstore/publications/Employment/EB_09-09-09.pdf#page=3>, from which this part of the discussion is adapted.

[126] *Id.*

[127] For example, the NLRB alleged in an unfair labor practices Complaint that a "Blogging and Internet Posting Policy" prohibiting employees "from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee's superiors, co-workers and/or competitors" was impermissibly broad and *per se* unlawful unless it carved out rights under the NLRA. *American Medical Response of Connecticut Inc. (AMR),* No. 34-CA-12576 (Complaint and Notice of Hearing, Oct. 27, 2010) <http://documents.jdsupra.com/daf37177-f935-4fe0-be1f-82c65d0f2ac3.pdf>. But the NLRB found that a different social-media policy adopted by retail giants Sears and K-Mart was not unlawful even though, in part, it forbade employees from disparaging the company's products, services, leadership, employees, strategy and business prospects. Given that provision "appears in a list of plainly egregious conduct, such as employee conversations involving the Employer's proprietary information, explicit sexual references, etc," it could not be construed as chilling protected activity in context and when reading the policy as a whole. *Sears Holdings*, No. 18-CA-19081 at 6 (Gen. Counsel Advice Mem. Dec. 4, 2009) <docstoc.com/docs/50764618/Sears-Holdings-%28Roebucks%29-18-CA-19081-120409>. *See also NLRB Settlement Agreement in the Matter of AMR of Connecticut, Inc.* (Feb. 7, 2011) <minnesotaemploymentlawreport.com/NLRB%20Facebook%20Settlement.pdf>. *See also* Walter Stella & Jessica Boar, *Social Media Policy After NLRB, Facebook Settlement*, The Recorder (Mar. 23, 2011) <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202487457090>.

Indeed, in the past couple years, the NLRB has increasingly targeted employers' social media restrictions as a potential infringement on concerted activity rights under the NLRA.[128] In April 2011, the NLRB's Acting General Counsel Lafe E. Solomon publicly staked out a forceful position that employees' social media activities can trigger federal labor law rights even for non-union employees,[129] and he added social media to the list of subjects in which he was taking particular interest.[130] Then, in August 2011, Solomon released a report concerning the outcomes of investigations into 14 respective NLRB social media cases from the preceding year.[131]

In late 2012, the Board in D.C. itself entered the fray, ruling that social-media posts can be protected concerted activity under the NLRA. On September 7, in *Costco Wholesale Corp. and United Food and Commercial Workers Union, Local 371,*[132] the Board issued its first decision on an employer's social media policy. Costco's policy prohibited employees from posting "statements … that damage the Company, defame any individual or damage any person's reputation." The Board invalidated the policy and ruled that it "clearly encompasse[d] concerted communications protecting [Costco's] treatment of its employees" without "even arguably suggest[ing] that protected communications are excluded."[133]

Then, a few weeks later, on September 28, 2012 the Board in D.C. issued its first decision involving adverse employment action based on a Facebook posting. There, in *Karl Knauz Motors, Inc. d/b/a Knauz BMW*, the NLRB found that an Illinois car dealer's firing of a salesman for photos and comments posted to his Facebook

---

[128] *See NLRB Continues String Of Actions Over Employee Use of Social Media*, Fenwick Emp. Brief (June 14, 2011) <fenwick.com/publications/6.5.4.asp?mid=71&WT.mcid=EB061411#NLRB>.

[129] Michael Starr and Katherine Healy Marques, *The NLRB's New Regulation of Social Media*, Nat'l L.J. (June 28, 2011) <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202498617574>.

[130] See the NLRB Memorandum here: <http://privacyblog.littler.com/uploads/file/NLRBMemorandumGC11-11.pdf>.

[131] NLRB Office of Public Affairs, *Acting General Counsel releases report on social media cases*, News Release (Aug. 18, 2011) <https://www.nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases>, linking to *Report of the Acting General Counsel Concerning Social Media Cases, Memorandum*, OM 11-74 (Aug. 18, 2011) <mynlrb.nlrb.gov/link/document.aspx/09031d458056e743>. *See also* John McLachlan, *Not As Bad As We Feared*, Fisher & Phillips LLP Labor Letter (Sep. 2011) <laborlawyers.com/showarticle.aspx?Show=14355&Type=1119&cat=3386&PrintPage=True>.

[132] *Costco Wholesale Corp. and United Food and Commercial Workers Union, Local 371,* 34–CA–012421 (Sept. 7, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580c45356>.

[133] *Costco Wholesale Corporation and United Food and Commercial Workers Union, Local 371,* 34–CA–012421 (Sept. 7, 2012) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580c45356>. *See* Mikal E. Belicove, *NLRB Slams Costco On Social Media Use Policy: What It Means For Your Business*, Forbes (Sept. 28, 2012) <http://www.forbes.com/sites/mikalbelicove/2012/09/28/nlrb-slams-costco-on-social-media-use-policy-what-it-means-for-your-business/>.

page did not violate federal labor law, because the activity was not concerted or protected.[134] The crux of the matter came down to whether the salesman was fired:

- exclusively for posting photos of and comments about an embarrassing and potentially dangerous accident at an adjacent Land Rover dealership also owned by his employer; and/or

- for posting mocking comments and photos with co-workers criticizing the employer's serving of hot dogs and bottled water at a luxury BMW car event.

The salesman had posted both sets of photos to Facebook on the same day; a week later, he was fired. The Board agreed with the Administrative Law Judge that the salesman was fired solely for the photos he posted of the Land Rover accident. The Board also agreed with the ALJ that the photos of the accident were "posted solely by [the employee], apparently as a lark, without any discussion with any other employee . . . and had no connection to any of the employees' terms and conditions of employment."[135]

In *Knauz*, The NLRB in D.C., through a two-Member majority, upheld the ALJ's decision that a "Courtesy" rule maintained by the employer regarding employee communications was unlawful. Its rationale was that employees would reasonably believe that the rule prohibited any statements of protest or criticism, even those protected by the NLRA. Dissenting, Member Brian E. Hayes found that the employer's rule was "nothing more than a common-sense behavioral guideline for employees" and that "[n]othing in the rule suggests a restriction on the content of conversations (such as a prohibition against discussion of wages)".[136]

Three days earlier, in a similar decision, an ALJ had invalidated EchoStar Technologies' social media policy that had prohibited employees from "disparaging" EchoStar or its affiliates and also prohibited employees from using personal social media with "EchoStar resources and/or on company time" absent company authorization.[137]

---

[134] *Karl Knauz Motors, Inc. d/b/a Knauz BMW*, 358 NLRB No. 164 at 4 (Sept. 28, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580ccba21>. *See also Knauz* Complaint (May 20, 2011) <hldataprotection.com/uploads/file/NLRB%20Complaint,%20Knauz%20BMW%20%285_20_11%29.pdf >, as ruled on in Case No. 13-CA-46452 (Lake Bluff, IL Sep. 28, 2011) <mynlrb.nlrb.gov/link/document.aspx/09031d4580683b21>.

[135] *Knauz,* NLRB No. 164 at 11 <mynlrb.nlrb.gov/link/document.aspx/09031d4580ccba21#page=11> (quoting *Knauz,* Case No. 13-CA-46452, at 9 <mynlrb.nlrb.gov/link/document.aspx/09031d4580683b21#page=9>).

[136] *Id.* at 4.

[137] *EchoStar Technologies*, 27-CA-066726, NLRB (Sept. 25, 2012) <mynlrb.nlrb.gov/link/document.aspx/09031d4580c8fc04>. For a discussion of the *Costco* and *EchoStar* decisions, *see* NLRB *Upholds Facebook Firing, But Strikes Down "Courtesy," Social Media, And Other Workplace Policie*s, Fenwick Employment Brief (Oct. 2012) <fenwick.com/publications/Pages/Fenwick-Employment-Brief-October-2012.aspx?WT.mc_id=EB_101712#nlrb>. *See also See* Beth P. Zoller, *Administrative Law Judge "Echos" NLRB's Most Recent Decisions on Social Media and Workplace Policies*, JD Supra (Oct. 8, 2012) <http://www.jdsupra.com/legalnews/administrative-law-judge-echos-nlrbs-11676/>.

At the tail end of 2012, the NLRB again invalidated parts of a social media policy, in *Dish Networks*.[138] There, consistent with its decision to invalidate the Costco defamation prohibition, the Board invalidated a provision prohibiting employees from making "disparaging or defamatory comments" about Dish and another prohibiting such behavior on "Company time." Applying the test outlined in Costco, the NLRB held that this language violated the NLRA by "banning employees from engaging in negative electronic discussion during 'Company time,'" and failing to clarify such discussion could occur during breaks and other non-working hours at the business. This decision further highlights the importance of a carefully drafted social media policy, with the assistance of legal counsel.

In the prior year or so, there had also been multiple other promulgations by ALJ's and by the NLRB GC. For example, firing employees for "harassment" when they engaged in a Facebook page discussion about working conditions and whether employees do enough to help their customers was found to have violated the NLRA protection of concerted activities, a holding upheld on appeal to the NLRB on December 14 2012.[139]

But when posts do not relate to the terms and conditions of employment, the NLRB has found no violation.[140] Moreover, in multiple cases involving employees posting disparaging comments about their supervisors or coworkers on Facebook, the conduct has not been deemed "concerted activity" because no other employees joined in the discussion or the intention of the post was not seen as attempting to initiate group action. For example, in one case an employee complained to her employer that a company accounting practice could constitute fraud, and then posted her belief on her Facebook page.[141]

The NLRB settlements and proceedings to date are non-conclusive as to where the pertinent boundaries may ultimately be drawn. Unfortunately, the NLRB's most recent Reports seem to create more confusion than clarity. In January 2012, Acting GC Solomon issued another report, covering 14 scenarios, seven of which involved social media, including Facebook and Twitter: NLRB Office

---

[138] *Dish Networks*, 359 NLRB No. 32 (Dec. 13, 2012) (Case No.16-CA-027316) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580e85dc6>. The ensuing summary is adapted from Daniel McCoy and Sheeva Ghassemi-Vanni, *NLRB continues to dissect employer social media policies* , Fenwick Emp. Brief (Dec, 18, 2012) <http://www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-December-2012.aspx#nlrb>.

[139] *See Hispanics United of Buffalo, Inc. and Carlos Ortiz, 359 NLRB No. 37* (Dec. 14, 2012) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580e8c5f4>, *affirming* Case 03–CA–027872 (Buffalo, NY Sep. 2, 2011) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580622877>. *See also* Complaint (May 17, 2011) <www.employmentlawmatters.net/uploads/file/5-17-11-Facebook%20firing-Hispanics%20United.pdf>.

[140] *Lee Enterprises d/b/a Arizona Daily Star*. Advice Memorandum (April 21, 2011) <www.employerlawreport.com/uploads/file/Lee%20Enterprises%20Advice%20Memo.pdf>.

[141] *See TAW, Inc.*, Case 26-CA-063082, GC Advice Memo (Nov. 22, 2011) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580755f55>, discussed in some detail in Brownstone eWorkplace II, supra note 2, at 59 (.pdf p. 64) <http://www.fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=64>.

of Public Affairs, *Acting General Counsel issues second social media report*, News Release (Jan. 25, 2012) <nlrb.gov/news/acting-general-counsel-issues-second-social-media-report>, linking to the report itself, *[Updated] Report of the Acting General Counsel Concerning Social Media Cases, Memorandum*, OM 12-31 (Jan. 24, 2012) <http://mynlrb.nlrb.gov/link/document.aspx/09031d45807d6567>.

Some of those 14 scenarios entailed allegations of a social-media policy overbroad on its face. Others addressed whether the given respective policies had been applied fairly. And still others involved both those concerns. NELI attendees and readers of this White Paper are urged to read the January 2012 Report to see if they can read the NLRB GC's tea leaves. This White Paper's author has read the Report multiple times and is still having a difficult time harmonizing the seemingly inconsistent results generated by the Report's analysis. Particularly troubling are the 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 the GC Report's suggestion that a compliant social-media policy contain multiple examples of contexts in which individual's posts or tweets 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. In sum, legal standards are still not settled as to which prohibitions would and would not constitute unfair labor practices.

On May 30, 2012, the NLRB Acting GC issued yet another report <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd>, summarized in this Alert written by colleagues of the author of this White Paper: Fenwick & West, *NLRB Issues Latest Memorandum On Social Media Policies*, Employment Brief (June 15, 2012) <www.fenwick.com/publications/Pages/Fenwick-Employment-Brief-June-2012.aspx?WT.mc_id=EB_061512#nlrb>. *See also* Jack Katzanek, *Social media guidelines favor employees*, Press-Enterprise (May 31, 2012) <http://www.pe.com/business/business-headlines/20120531-workplace-social-media-guidelines-favor-employees.ece>.

The May 2012 report addressed seven social media policies that collectively highlight how the NLRB defines "protected concerted activity" under Section 7 of the

National Labor Relations Act (NLRA) as it applies to employees' use of social media.[142] Many commentators have noted that a common theme in the NLRB's advice to employers is to provide employees with clear information, context, and examples in social media policies.[143] Some have criticized the recent NLRB social media guidance for companies on designing social media policies as "overbroad,"[144] and others have noted that employers revising their social media guidelines should be aware of how changes in those policies may affect internal reporting procedures and policies.[145]

Although not in the social-media context, *compare Plaza Auto Center, Inc. v. NLRB*, 664 F.3d 286 (9th Cir. 2011) (remanding on some issues but agreeing with ALJ and Board

---

[142] Office of General Counsel Memorandum OM 12-59 (May 30, 2012) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd>. For a summary of the underlying social media policies and the NLRB's analysis, *see* M. Michael Cole, *Specificity Gets the Nod from the NLRB*, The Recorder (June 8, 2012) ("[a] common theme emerges from the board's discussion and provides employers with important drafting guidance[; i]n particular, employer policies, practices and rules that contain no limiting language or context to clarify to employees what conduct is prohibited will likely run afoul of the NLRA") <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202558734701>; Alex Stevens, *NLRB'S General Counsel Releases New Social Media Report Containing Much Needed Guidance on Lawful Social Media Policies*, Social Media Law Brief (June 20, 2012) ("[a] key takeaway from this report is the importance of using examples to clarify what types of behavior are prohibited") <http://blogs.haynesboone.com/index.php/2012/06/firm/some/nlrbs-general-counsel-releases-new-social-media-report-containing-much-needed-guidance-on-lawful-social-media-policies/>. For a brief analysis of recent NLRB decisions, see Abigail Rubenstein, *5 Tips For a Social Media Policy that Won't Rile the NLRB*, Law 360 (Oct. 22, 2012) <http://www.law360.com/articles/388109/5-tips-for-a-social-media-policy-that-won-t-rile-the-nlrb>.

[143] *See id.* Note that courts are similarly aware of the need to provide explicit instructions to jurors about their use of social media. *See, e.g. Proposed Model Jury Instruction: The Use of Electronic Technology to Conduct Research on or Communicate about a Case*, Prepared by the Judicial Conference Committee on Court Administration and Case Management (June 2012) ("I know that many of you use cell phones, Blackberries, the internet and other tools of technology. You also must not talk to anyone at any time about this case or use these tools to communicate electronically with anyone about the case. This includes your family and friends. You may not communicate with anyone about the case on your cell phone, through e-mail, Blackberry, iPhone, text messaging, or on Twitter, through any blog or website, including Facebook, Google+, My Space, LinkedIn, or YouTube. You may not use any similar technology of social media, even if I have not specifically mentioned it here. I expect you will inform me as soon as you become aware of another juror's violation of these instructions.") <http://legaltimes.typepad.com/files/model-jury-instructions.pdf>.

[144] Jaclyn Jaeger, *Latest NLRB Social Media Guidance Draws Criticism,* Compliance Week (June 26, 2012) <http://www.complianceweek.com/latest-nlrb-social-media-guidance-draws-criticism/printarticle/246425/> (subscription may be required).

[145] Doreen S. Davis and Ann Marie Painter, T*he NLRB's View on Reporting Workplace Concerns via Social Media*, Corporate Counsel (August 13, 2012) ("employers should ensure that, in the process of modifying their social media policies to address the Board's [NLRA] Section 7 concerns, they do not weaken existing internal policies for the reporting of possible discrimination, harassment, and/or retaliation in the workplace and foreclose the options not only of prompt remediation but also of the assertion of the important and valuable *Faragher/Ellerth* defense.") <http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202567007227&The_NLRBs_View_on_Reporting_Workplace_Concerns_via_Social_Media>.

that employee's verbal outburst was protected "because [it] was contemporaneous with [the employer's] censure of [his] protected activities as 'a lot of negative stuff'' and [the employer's] unfair labor practice of suggesting that [he[could work elsewhere if he did not like the company's policies") <www.ca9.uscourts.gov/datastore/opinions/2011/12/19/10-72728.pdf>, as discussed in Alan S. Levins, *On-the-Job-Tirades*, Cal. Lawyer (July 2012) <www.callawyer.com/common/CLprint.cfm?eid=923332&evid=1>.

One other odd NLRB development in 2012 occurred in the I-9 context. A March 22, 2012 NLRB settlement with Pacific Steel Casting Company signals that , "[w]hen considering voluntary enrollment in the E-Verify Program, organizations with a unionized workforce must review their collective bargaining agreements to ensure that enrollment does not violate contract provisions or other bargaining responsibilities." Ann Cun, *NLRB Settlement – Know When to Enroll in E-Verify*, The I-9 and E-Verify Blog (Apr. 19, 2012) <http://www.lawlogix.com/electronic-i9/everify/nlrb-settlement-know-when-to-enroll-in-e-verify/>.

In any event, the NLRB's vigorous activity in the Web 2.0 arena may or may not be a harbinger of similar unfair labor practice complaints brought by public sector employees. 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.

C. Risks of Strict Policies

1. Creation of Duty to Act?

An employer's *right* to monitor must be distinguished 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 an employee's harmful activities plus the employer's failure to remedy the behavior. For more on this issue, *see* Brownstone eWorkplace II, supra note 2, at 60 (.pdf pp. 65) @ n. 270 <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=58>.

2. Prohibit Innocent Surfing?

An employer, however, should be cautious of having overbroad web-surfing restrictions, especially if it only plans to enforce such limits selectively.[146] As noted in Takeaway # 6 at page 15 above, one viable option is to craft policies so that they evince a rule-of-reason – namely acknowledging that employees may engage in incidental personal use of the Internet as long as such use does not interfere with the employee's duties.

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

D. Periodic Training

Some identify the fundamental principles of policy implementation as "The Three E's," namely Establish, Educate and Enforce.[147] Anyway, having developed written policies, employers should not only provide periodic training on the contents of such policies but also strive to enforce the underlying principles consistently.[148]

E. Information-Security Compliance Considerations

For an overview of this area, *see* the same two items cited in sub-section V(D) immediately above. For more resources, *see* the author's extensive Bibliography at <http://www.fenwick.com/professionals/Pages/bobbrownstone.aspx>.

Encryption of data in transit and at rest should always be a high priority, especially on laptops. The recent NASA situation, discussed at notes 14 and _-_ and accompanying text above, is a stark reminder of the dire consequences can result when unencrypted PII is on a stolen or lost laptop.

---

[147] Dunn, Darrell, *Email is Exhibit A*, Information Week (May 8, 2006) (citing ePolicy Institute) <informationweek.com/shared/printableArticle.jhtml;jsessionid=JVK0JEBYYBRZWQSNDLRSKH0CJUNN2JVN?articleID=187200562&_requestid=12387>.

[148] Lothar Determann and Ute Krudewagen, *Policing Social Media*, Recorder (Apr. 6, 2012) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202548286075>; 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) <http://www.dinsmore.com/regulating_employee_personal_conduct>. *See also* Brownstone eWorkplace II, supra note 2, at 61 <fenwick.com/FenwickDocuments/eWorkplace_Privacy_Social-Media_Materials_NELI_Brownstone_4-3-12.pdf#page=66> and Brownstone eWorkplace I, at 82-85 <fenwick.com/fenwickdocuments/eworkplace_policies_materials_public_sector_eeo_8-28-09.pdf#page-82>.

APPENDIX A

Robert D. Brownstone – Materials & Resources –

SAMPLE SOCIAL-MEDIA POLICIES – @ 2/8/13

- ***Web-2.0/Social-Media Policies –Samples:***
  - ***Private Sector***:
    - 219 Policies in database at <http://socialmediagovernance.com/policies.php>
    - <http://op.bna.com/pl.nsf/id/dapn-7vak72/$File/AP.pdf> (AP's Social-Media "Q&A")
    - Walmart Policy (5/4/12) approved by NLRB ***(BUT INCONSISTENT WITH NLRB CONCERNS)***:
      - Policy itself: <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd#page=22>
      - NLRB Commentary: *Id.* at 1 and 19-20
    - <www.delawareemploymentlawblog.com/Sample%20Social%20Media%20Policy%20YCST.pdf> (linked from <www.delawareemploymentlawblog.com/2011/10/sample-socialmedia-policy.html>)
    - <www.ibm.com/blogs/zz/en/guidelines.html> ("IBM Social Computing Guidelines")
    - <immagic.com/eLibrary/ARCHIVES/GENERAL/IBM/I070811V.pdf> ("IBM Virtual World Guidelines")
    - <http://www.law.com/jsp/tal/PubArticleTAL.jsp?id=1202426674355>, linking to sample:
      - <http://shorl.com/mogustemymidru> (Jaffe PR Sample; revised 11/7/12)
    - <http://www.lehrmiddlebrooks.com/SocialMedia.html>
    - <www.epolicyinstitute.com/bin/loadpage.cgi?1254863981+forms/index.asp> ($99)
    - <www.messagelabs.com/white_papers/epolicy_form> (free registration)
  - ***Public Sector (some also addressing Public-Records issues)***:
    - <www.records.ncdcr.gov/guides/best_practices_socialmedia_stateagency_finalv2_20120307.pdf>
    - <www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2012>
    - <va.gov/vapubs/viewPublication.asp?Pub_ID=551&FType=2>
    - <http://www.cio.ca.gov/Government/IT_Policy/pdf/ITPL_10-02_Social_Media.pdf> OR <http://www.cio.ca.gov/Government/IT_Policy/msdoc/ITPL_10-02_Social_Media.doc>
    - <cms.oregon.gov/DAS/ETS/EGOV/BOARD/pages/social_networking_guide/public_records.aspx>
    - <http://www.texas.gov/en/about/Pages/social-media-policy.aspx>
    - <www.utahta.wikispaces.net/file/view/State+of+Utah+Social+Media+Guidelines+9.29.pdf>
    - <http://www.mrsc.org/subjects/infoserv/socialmedia.aspx> (Washington state – cities)
    - <http://www.seattle.gov/pan/SocialMediaPolicy.htm>

(c't'd)

- ***Related Helpful Resources***

  - ***Private Sector***:

    - 178 Reports at <http://socialmediagovernance.com/studies/>
    - <http://www.delawareemploymentlawblog.com/social-media-in-the-workplace/>
    - Baker & McKenzie, *The Social Media Issue*, The Global Employer (Sep. 25, 2012) (addressing U.S. plus 16 other countries) <http://www.bakermckenzie.com/files/Publication/fbb96048-99a8-49f0-9d4f-f612e0bec1c0/Presentation/PublicationAttachment/2ee3b2aa-40e1-4612-93b8-03b7ee1feddb/bk_employment_globalemployersocialmedia_sep12.pdf>
    - <http://www.delawareemploymentlawblog.com/privacy-in-the-workplace/>
    - <http://mashable.com/2009/04/28/facebook-privacy-settings>
    - <http://www.bicklaw.com/Publications/LAWFULMININGOFSOCIALNETWORKS.htm>

  - ***Public Sector (some also addressing Public-Records issues)***:

    - <http://www.epa.gov/irmpoli8/policies/respond.pdf>
    - <http://www.records.ncdcr.gov/> (North Carolina's very helpful, intense materials)
    - <www.youtube.com/playlist?list=PLEA6C999DEB82E2FC> (NC: 5-part video series)
    - <http://mashable.com/2012/07/30/public-sector-social-media/>
    - <http://www.businessofgovernment.org/sites/default/files/Social%20Media%20Strategy%20Brief_0.pdf>
    - <http://www.businessofgovernment.org/sites/default/files/A%20Managers%20Guide%20for%20Using%20Twitter%20in%20Government.pdf>
    - <http://archivesocial.com/blog/social-media-public-records> (quoting above NC, Oregon & Texas policies)
    - <http://armylive.dodlive.mil/index.php/2012/06/social-media-handbook-edition-3/>
    - <http://www.archives.nysed.gov/a/records/mr_social_media.shtml>
    - <http://archives.utah.gov/documents/social-media-guidelines_2011.pdf>

Appendix B – Social-Media eDiscovery – Brownstone Bibliography (3/4/13)

SOME Social-Media eDiscovery Decisions

- *Lineberry v. Richards*, 2013 WL 438689, 20 Wage & Hour Cas.2d (BNA) 359 **(E.D. Mich. 2/5/13)** (where Facebook posts of Mexico vacation had landed employee on FMLA leave in hot water, finding that "[b]ased on such undisputed dishonesty, [the employer] had a right to terminate [the employee] – without regard to her leave status because the FMLA does not afford an employee greater rights than she would have if . . . not on FMLA leave") <http://www.gpo.gov/fdsys/pkg/USCOURTS-mied-2_11-cv-13752/pdf/USCOURTS-mied-2_11-cv-13752-0.pdf>

- *Keller v. National Farmers Union Property & Cas. Co.*, 2013 WL 27731, at *4 **(D. Mont. Jan 2, 2013)** (in personal injury action, finding Defendant "not entitled to delve carte blanche into the nonpublic sections of Plaintiffs' social networking accounts" absent making "the requisite threshold showing" that the desired information within scope of discovery) <http://docs.justia.com/cases/federal/district-courts/montana/mtdce/9:2012cv00072/41571/22/0.pdf?1357219232>

- *Reid v. Ingerman Smith LLP*, 2012 WL 6720752 **(E.D.N.Y. Dec. 27, 2012)** (requiring same-sex harassment Plaintiff to produce non-public postings (including as to social activities) from her Facebook account based on defense contention that public postings revealed information contradicting mental anguish claims) <http://docs.justia.com/cases/federal/district-courts/new-york/nyedce/1:2012cv00307/326380/33/0.pdf?ts=1356693028>

- *Richards v. Hertz Corp.*, 100 A.D.3d 728, 953 N.Y.S.2d 654, 656 **(N.Y. A.D. 2 Dep't Nov. 14, 2012)** (in personal injury case, affirming potential discoverability of – and order of *in camera* review regarding – one Plaintiff's Facebook private "status reports, e-mails, and videos that – might be] relevant to the extent of her alleged injuries" <www.courts.state.ny.us/courts/ad2/calendar/webcal/decisions/2012/D34155.pdf>

- *E.E.O.C. v. Original Honeybaked Ham Co. of Georgia*, 2012 WL 5430974, 116 Fair Empl.Prac.Cas. (BNA) 743, 96 Empl. Prac. Dec. ¶ 44,675 **(D. Colo. Nov. 7, 2012)** (in harass-ment case, ordering broad discovery from class of 20+) <docs.justia.com/cases/federal/district-courts/colorado/codce/1:2011cv02560/128657/241/0.pdf?ts=1352370474>, followed by court-ordered questionnaire **(D. Colo. Jan. 9, 2013)** <docs.justia.com/cases/federal/district-courts/colorado/codce/1:2011cv02560/128657/285/0.pdf?ts=1357819204>

- *In re White Tail Oilfield Services, L.L.C.*, 2012 WL 4857777 **(E.D. La. Oct. 11, 2012)** (in personal injury case, finding discoverability of all of individual's live and "deleted" data obtainable from Facebook's "Download Your Information" feature) <http://docs.justia.com/cases/federal/district-courts/louisiana/laedce/2:2011cv00009/144679/144/0.pdf?1350040204>

- *Howell v. Buckeye Ranch*, 2012 WL 5265170, at *1 **(S.D. Ohio Oct. 2, 2012)** (in sexual harassment case, Defendants not entitled to Plaintiff's Facebook login and password but *were* "free to . . . seek information from [her social-media accounts . . . [;] Plaintiff's counsel can then access the private sections of [her] accounts and provide [responsive] information and documents") <www.technologylawsource.com/uploads/file/HowellvTheBuckeeRanchInc.pdf>.

- *Glazer v. Fireman's Fund*, 2012 WL 1197167, at *3 **(S.D.N.Y. Apr. 5, 2012)** (directing discrimination/retaliation Plaintiff herself to gather and produce her chats in her LivePerson account; circumventing SCA/privacy concerns Plaintiff raised as to direct production from social-media site purveyor) <http://scholar.google.com/scholar_case?case=13277180327682826171>

SOME Social-Media eDiscovery Decisions *(c't'd)*

- *Danielle 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)** <gibbonslaw.com/files/1349899536.pdf>

- *Robinson v. Jones Lang LaSalle Americas*, *Inc.*, 2012 WL 3763545 **(D. Ore., Aug. 29, 2012)** <www.ediscoverylaw.com/uploads/file/Robinson%20v%20Jones%20Lang%20LaSalle.pdf>

- *U.S. v. Meregildo*, --- F.Supp.2d ----, 2012 WL 3264501, at *2 **(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'") <saltlakecriminaldefense.com/wp-content/uploads/2012/08/US-v.-Meregildo-FB-4th-Amend-Case.pdf>

- *Coates v. Mystic Blue Cruises, Inc.* 2012 WL 3860036, at *2 **(N.D. Ill. Aug. 9, 2012)** (in sexual harassment suit, allowing use of redacted versions of some of Plaintiff's social-media communications only for possible impeachment) <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2011cv01986/253804/80/0.pdf?1344639157>

- *Targonski v. City of Oak Ridge*, 2012 WL 2930813, at *8, *10 **(E.D. Tenn. July 18, 2012)** (in finding that hostile environment claim survived summary judgment motion, ruling that Plaintiff's Facebook posts admissible at trial so jury could assess Defendant's theory that "workplace rumors [were not] offensive when she herself was making similar statements") <http://docs.justia.com/cases/federal/district-courts/tennessee/tnedce/3:2011cv00269/61052/22/0.pdf?1342726854>

- *Thompson v. Autoliv ASP, Inc.*, 2012 WL 2342928, at *4 **(D. Nev. June 20, 2012)** (in personal injury action, "[b]ecause the alleged consequences of Plaintiff's injuries include[d] severe physical injuries, emotional distress, and impaired quality of life, evidence relating to Plaintiff's physical capabilities and social activities is relevant to Plaintiff's claims in this action.") <www.ediscoverylaw.com/uploads/file/Westlaw_Document_Thompson.doc>

- *Juror No. One v. Superior Court (Royster)*, 206 Cal. App. 4th 854, 142 Cal. Rptr. 3d 151, 153 **(Cal. App. 3 Dist. May 31, 2012)** (upholding "order requiring [j]uror . . . to execute [SCA] consent form . . . authorizing Facebook to release to the court for in camera review all items he posted during [criminal] trial") <http://www.courts.ca.gov/opinions/documents/C067309.PDF>

- *Davids v. Novartis Pharmaceuticals Corp*., No. CV06-0431 **(E.D.N.Y. Feb. 24, 2012)** <http://www.newyorkpersonalinjuryattorneyblog.com/NYPIAB/wp-content/uploads/2012/02/FacebookDecision-Judge-Wall.pdf>

- *Tienda v. State*, 358 S.W.3d 633 **(Tex. Crim. App. Feb. 8, 2012)** (circumstantial evidence sufficient to authenticate MySpace postings) <cca.courts.state.tx.us/OPINIONS/PDFOPINIONINFO2.ASP?OPINIONID=22068>

- *People v. Valdez*, 201 Cal. App. 4th 1429, 1434-1437 **(Cal. App. 4th Dist. Dec. 16, 2011)** (section on authentication not published; holding reasonable trier of fact could conclude from posting of personal photographs, communications and details social media profile belonged to Defendant) <leagle.com/xmlResult.aspx?page=2&xmldoc=In%20CACO%2020111216048.xml&docbase=CSLWAR3-2007-CURR&SizeDisp=7>.

- *Largent v. Reed*, No. 2009-1823 **(Pa. Ct. Common Pleas Franklin Cty. Nov. 8, 2011)** <http://druganddevicelaw.net/Opinions%20in%20blog/Largent.pdf>

SOME Social-Media eDiscovery Decisions *(c't'd)*

- *Lester v. Allied Concrete Co.*, Nos. CL.08-1S0 & CL09-223 **(Va. Cir. Ct. Charlottesville)**:
    - **Oct. 21, 2011 Order** (spoliation sanctions: $542,000 against Plaintiff's counsel; and $180,000 against Plaintiff) <x1discovery.com/download/Lester_v_Allied_Concrete_Final_Order.pdf>
    - **Sep. 1, 2011 Opinion** (spoliation finding and damages remittitur in wrongful death case where counsel had instructed surviving spouse to "clean up" his social-media pages during lawsuit) <valawyersweekly.com/vlwblog/files/2011/09/Lester-Hogshire-order.pdf>
- *Quagliarello v. Dewees*, 2011 WL 3438090 **(E.D. Pa. Aug. 4, 2011)** ("Memorandum re: Motions in Limine") <http://www.technolawyer.com/litigationworld/d/quagliarello080412.pdf>
- *Griffin v. State*, 19 A. 3d 415 **(Md. Ct. App. Apr. 28, 2011)** (birth date and photo insufficient to authenticate printout of MySpace profile) <http://mdcourts.gov/opinions/coa/2011/74a10.pdf>
- *Romano v. Steelcase*, 907 N.Y.S. 2d 650, at *5 **(N.Y. Sup. Sep. 21, 2010)** <courts.state.ny.us/Reporter/3dseries/2010/2010_20388.htm>
- *McMillen v. Hummingbird Speedway, Inc*., No. 113-2010 CD **(Pa. C.P. Jefferson Cty. Sep. 9, 2010)** <ediscoverylaw.com/uploads/file/McMillen%20v%20Hummingbird%20Speedway.pdf>
- *Barnes v. CUS Nashville, LLC, [d/b/a Coyote Ugly Saloon]*, 2010 WL 2265668 **(M.D. Tenn. June 3, 2010)** <https://ecf.tnmd.uscourts.gov/doc1/16911303989>
- *Crispin v. Christian Audigier, Inc.*, No. CV 09-09509 MMM (JEMx) **(C.D. Cal. May 26, 2010)** <ecf.cacd.uscourts.gov/doc1/031110245153>
- *E.E.O.C. v. Simply Storage Management, LLC*, 270 F.R.D. 430, 434 **(S.D. Ind. May 11, 2010)** (social-networking site "content is not shielded from discovery simply because it is 'locked' or 'private'[;] and "must be produced when it is relevant to a claim or defense") <iediscovery.com/files/Simply_Storage.pdf>
- *U.S. v. Phaknikone*, 605 F.3d 1099, 1107 **(11th Cir. May 10, 2010)** <ca11.uscourts.gov/opinions/ops/200910084.pdf>
- *Nguyen v. Starbucks Coffee Corp.*, 2009 WL 4730899 **(N.D. Cal. Dec, 7, 2009)** <https://ecf.cand.uscourts.gov/doc1/03516287723>
- *Bass ex rel. Bass v. Miss Porter's School*, 2009 WL 3724968 **(D. Conn. ct. 27, 2009)** <http://docs.justia.com/cases/federal/district-courts/connecticut/ctdce/3:2008cv01807/83529/142/0.pdf?1270119115>
- *Quigley Corp. v. Karkus*, 2009 WL 1383280 **(E.D. Pa. May 15, 2009)** <http://www.paed.uscourts.gov/documents/opinions/09d0568p.pdf>
- *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 **(D. Colo. Apr. 21, 2009)** <http://docs.justia.com/cases/federal/district-courts/colorado/codce/1:2006cv01958/98669/179/0.pdf?ts=1270625074>
- *Dexter v. Dexter,* 2007 WL 1532084 **(Ohio Ct. App. May 25, 2007)** (award of custody to father due to mother's blog posts as to sadomasochism, bisexuality and paganism) <www.sconet.state.oh.us/rod/newpdf/11/2007/2007-ohio-2568.pdf>
- *In the Interest of T.T.,* 228 S.W.3d 312 **(Tex. App. May 17, 2007)** (affirming termination of parental rights in part because of myspace post 'I don't want kids'") <http://caselaw.findlaw.com/tx-court-of-appeals/1299520.html>
- *Mackelprang v. Fidelity National Title Agency of Nevada*, 2007 U.S. Dist. LEXIS 2379 **(D. Nev. Jan. 9, 2007)** <https://ecf.nvd.uscourts.gov/doc1/11511167020>

Appendix B – Social-Media eDiscovery – Brownstone Bibliography (3/23/13)

eDiscovery-Law Online Libraries (& alerts/advance-sheets)

- Applied Discovery, *Law Library* <http://www.applieddiscovery.com/ws_display.asp?filter=Online%20Law%20Library>
    - *Case Law Summaries* <www.applieddiscovery.com/ws_display.asp?filter=Case%20Summaries>
    - *ByTopic* <www.applieddiscovery.com/ws_display.asp?filter=View%20By%20Topic>
    - *By Jurisdiction* <www.applieddiscovery.com/ws_display.asp?filter=View%20By%20Jurisdiction>
- K&L, Gates *Blog, etc.* <http://www.ediscoverylaw.com/>
    - *Case Law Database* <https://extranet1.klgates.com/ediscovery/>
- Kroll, OnTrack Data, *Resource Library* <http://www.krollontrack.com/resource-library/>
    - *Case Law Database* (searchable by topic or jurisdiction) <www.krollontrack.com/resource-library/case-law/>
        - *Static List -- by Topic* <www.krollontrack.com/library/topic.pdf> (last updated 7/9/12)
        - *Static List -- by Jurisdiction* <www.krollontrack.com/library/jurisdiction.pdf> (last updated 7/9/12)
- Law Technology News, *e-discovery & compliance news* <law.com/jsp/lawtechnologynews/e_discovery.jsp>

eDiscovery-Law Blogs, etc.

- *Bow Tie Law's Blog* <http://bowtielaw.wordpress.com>
- *eDiscovery Insights* <http://www.ediscoverycalifornia.com>
- *eDiscovery Journal (eDJ)* <http://ediscoveryjournal.com/>
- *eDiscovery Search Blog* <http://www.catalystsecure.com/blog/author/bob-ambrogi>
- *eDiscovery Team Blog* <http://e-discoveryteam.com/>

eDiscovery LinkedIn Groups

- Association of Certified E-Discovery Specialists (ACEDS) <www.linkedin.com/groups?gid=3004904>
- eDiscovery Networking Group <www.linkedin.com/groups?gid=126929>
- eDiscovery People <www.linkedin.com/groups/eDiscovery-People-3863091>
- eDiscovery Readiness for Government <www.linkedin.com/groups?gid=2729942>

eDiscovery and Forensics Online Glossaries *(also Brownstone's Glossary available on request)*

- <http://www.applieddiscovery.com/e-discovery-terminology.html>
- <http://www.edrm.net/resources/glossary>
- <http://Fios-Glossary.notlong.com>
- <http://www.krollontrack.com/resource-library/glossary/>
- <http://www.thesedonaconference.org/content/miscFiles/glossary2010.pdf> (free registration required)
- <http://viaforensics.com/education/computer-forensics-ediscovery-glossary/>

Computer Technology Terminology Online Glossaries

- How Stuff Works <http://electronics.howstuffworks.com/tech>
- Matisse's Glossary of Internet Terms <http://www.matisse.net/files/glossary.html>
- Spyware "Words to Know" (*free registration required*) <http://Spyware-Glossary.notlong.com>
- Techsoup (*free registration required*) <http://www.techsoup.org/>
- TechWeb TechEncyclopedia <http://www.techweb.com/encyclopedia/>
- Webopedia <http://www.webopedia.com/>
- WhatIs.com <http://whatis.techtarget.com/>

eDiscovery Law Review Trilogy by Robert Brownstone

- *Preserve or Perish; Destroy or Drown – eDiscovery Morphs Into EIM*, 8 N.C.J. L. & Tech. (N.C. JOLT), No. 1, at 1 (Fall 2006) <web.archive.org/web/20100703000846/http:/jolt.unc.edu/sites/default/files/8_nc_jl_tech_1.pdf>, as updated by 2007 Supplement <fenwick.com/docstore/publications/EIM/NC_JOLT_eDiscovery_Supplement.pdf>
- *Collaborative Navigation of the Stormy e-Discovery Seas*, 10 Rich. J.L. & Tech. 53 (2004) <http://law.richmond.edu/jolt/v10i5/article53.pdf>
- *EDiscovery: Preserving, Requesting & Producing Electronic Information*, 19 Santa Clara Computer & High Tech. L.J. 131 (2002) (co-author) <fenwick.com/docstore/publications/Litigation/ediscovery.pdf>

Metadata Bibliography by Robert Brownstone (8/23/12)

- <http://www.fenwick.com/FenwickDocuments/Brownstone_Metadata_Bibliography.pdf>

Full Brownstone Bibliography ***(incl. eDiscovery articles, slide decks & press-quotes)***

- <fenwick.com/bobbrownstoneinsights>

APPENDIX C – Brownstone – Resources re: Attorney-Client Privilege, etc. (2/2/13)

I. Attorney-Client Privilege Opinions

- *U.S. v. Hamilton*, 701 F.3d 404, 408-09 **(4th Cir. 12/13/12)** ("waiver of marital privilege by email usage [where employee] did not take any steps to protect the emails in question, even after he was on notice of his employer's policy permitting inspection of emails stored on the system at the employer's discretion") (citing below *Simons* and *Global Crossing* attorney-client privilege decisions) <http://www.ca4.uscourts.gov/Opinions/Published/114847.P.pdf>

- *Aventa Learning*, *Inc. v. K12, Inc.*, 2011 WL 5438960, at *19 **(W.D. Wash. 11/8/11)** ("[b]ased on the company policy . .. [terminated senior level manager] could not have had a reasonable expectation of confidentiality with regard to communications or other materials that he created or received on his [employer-issued] laptop") <http://shorl.com/hugrajugutrehu>

- *Hanson v. First Nat'l Bank*, 2011 WL 5201430, at *6 **(S.D. W. Va. 10/31/11)** (former officer, "knowing that [his then-employer] could access and monitor his email communications with his criminal attorney, had no objectively reasonable expectation of privacy or confidentiality in them and effectively waived the attorney-client privilege in using [employer-provided] computer system in communicating with his criminal attorney.) <http://docs.justia.com/cases/federal/district-courts/west-virginia/wvsdce/5:2010cv00906/65843/126/0.pdf>

- ABA Formal Opinions 11-459 & 11-460 (**ABA 8/4/11**):
  - *Duty to Protect the Confidentiality of E-mail Communications with One's Client* <www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf>
  - *Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel* <www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_460_nm_formal_opinion.authcheckdam.pdf>

- *Taylor v. Waddell & Reed, Inc.*, 2011 WL 1979486, * 1 n.2, 2011 U.S. Dist. LEXIS 54109, *6 n.2 (**S.D. Cal. 5/20/11**) ("Plaintiffs concede that no Financial Advisors had an expectation of privacy in the contents of any e-mail sent using Defendant's e-mail system") <http://docs.justia.com/cases/federal/district-courts/california/casdce/3:2009cv02909/313120/108/0.pdf>

- *In re Royce Homes, LP*, 449 B.R. 709 (**Bkrtcy. S.D. Tex. 3/11/11**) ("Debtor's guidelines on monitoring were so explicit and straightforward that no employee could reasonably believe the Debtor would not or could not view his or her personal e-mails") <http://blog.mclane.com/wp-content/uploads/2011/09/In-re-Royce-Homes-LP.pdf>

- *Holmes v. Petrovich*, 191 **Cal. App.** 4th 1047, 119 Cal. Rptr. 3d 878 (**3 Dist. 1/13/11**) (no privilege as to communications sent via work email system because employee knew of TAUP as to no personal use, had notice that company would monitor and was warned of NoEEP) <http://caselaw.findlaw.com/ca-court-of-appeal/1552780.html>

- *DeGeer v. Gillis*, 2010 WL 3732132 (**N.D. Ill. 9/17/10**) (no waiver; "[b]ecause the record does not contain [employer']s computer usage policy, . . . [I] cannot determine whether [it] prohibited employees from using their company computers to conduct personal legal matters") <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2009cv06974/237454/122/0.pdf>

- *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 108 Fair Empl .Prac. Cas. (BNA) 1558 (**N.J. 3/30/10**) <http://lawlibrary.rutgers.edu/collections/courts/supreme/a-16-09.opn.html>, ***affirming and modifying*** 408 N. J. Super. 54, 973 A.2d 390, 393, 106 Fair Empl. Prac. Cas. (BNA) 1177, 158 Lab. Cas. ¶ 60,829, 29 IER Cases 588 (N.J. App. Div. 6/26/09) ("policies undergirding the attorney-client privilege substantially outweigh the employer's interest in enforcement of its unilaterally imposed regulation; reject[ing] employer's claimed right to rummage through and retain the employee's emails to her attorney") <http://lawlibrary.rutgers.edu/collections/courts/appellate/a3506-08.opn.html>, ***reversing*** 2009 WL 798044 (N.J. Super. L. Div. 2/5/09) <privacyblog.littler.com/uploads/file/Stengart%20v%20Loving%20Care.pdf>

- *Convertino v. U.S. DOJ*, 674 F. Supp. 2d 97 (**D.D.C. 12/10/09**) (applying New York Law to uphold reasonable expectation of privacy of federal prosecutor employed by U.S. DOJ) <https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2004cv0236-167>.

- *United States v. Hatfield*, 2009 U.S. Dist. LEXIS 106269, *26-27 (**E.D.N.Y. Nov. 13, 2009**) (despite Policy's express warnings that employees should use their computers solely for "business purposes" and "should not assume that any computer equipment or technologies such as electronic mail and data are confidential or private," holding that defendant did not waive attorney-client privilege or work product doctrine as to documents stored on his office computer) <http://www.orrick.com/fileupload/2265.pdf>

I. Attorney-Client Privilege Opinions *(c't'd)*

- *Alamar Ranch, LLC v. County of Boise*, 2009 U.S. Dist. LEXIS 101866, 2009 WL 3669741 (**D. Idaho 11/2/09**) (pro-employer/subpoena recipient; e-mails to and from lawyer as opposed to cc's to lawyer; FHA case) <http://www.steptoe.com/assets/attachments/3958.pdf>

- *Leor Exploration & Prod. LLC v. Aguiar***,** 2009 WL 3097207 (**S.D. Fla. 9/23/09**) (finding ex-employee "invoking the attorney-client privilege . . . ha[d] not met . . . burden because [had] not shown a reasonable expectation of privacy in emails transmitted through [employer]'s server") <http://myfloridalegal.com/alerts.nsf/0/512bcf66e297c698852577060059c0a2/$FILE/Leor.pdf>

- *Fiber Materials, Inc. v. Subilia*, 974 A.2d 918 (**Me. 7/16/09**) (split between pro-employee majority and pro-employer concurring opinions) <http://caselaw.findlaw.com/me-supreme-judicial-court/1234210.html>

- *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 587 F. Supp. 2d 548 **(S.D.N.Y. 10/23/08)** <https://ecf.nysd.uscourts.gov/doc1/12715425216> (adopting Magistrate's 51 pp. Report and Recommendation (Aug.22, 2008), available at <https://ecf.nysd.uscourts.gov/cgi-bin/show_doc.pl?caseid=326754&de_seq_num=255&dm_id=4941830&doc_num=70&pdf_header=1>)

- *Scott v. Beth Israel Medical Ctr.*, 17 N.Y. Misc. 3d 934, 2007 N.Y. Slip Op. 27429 (**N.Y. Sup. N.Y. 10/17/07**) (in employment contract action; Plaintiff's communications with attorney as to litigation, transmitted over Defendant's email system, not protected by privilege or work-product, in light of "no personal use" and monitoring policies) <nycourts.gov/reporter/3dseries/2007/2007_27429.htm>

- *Sims v. Lakeside School*, 2007 WL 2745367, 2007 U.S. Dist. LEXIS 69568 (**W.D. Wash. 9/20/07**) ("clear [contents of] policy " partially trumped by "public policy" such that employer "not permitted to review any web-based generated e-mails, or materials created by plaintiff . . . to communicate with his counsel or his wife") <http://www.internetlibrary.com/pdf/Chance-Sims-Lakeside-School-WD-Wash.pdf>

- *Transocean Capital v. Fortin*, 21 Mass. L. Rptr. 597, 2006 WL 3246401 (Mass. Super. Ct. Oct. 20, 2006) (though finding waiver for other reasons, finding employer had not shown it actually adopted HR policies administered by third-party provider – such that mere "us[e of] Company's email address and … system" insufficient to waive privilege) <masslawyersweekly.com/fulltext-opinions/2006/10/23/transocean-capital-inc-v-fortin-et-al/>

- *Long v. Marubeni America*, 2006 WL 2998671, at *1, *3 (**S.D.N.Y. 10/19/06**) (where temporary internet files contained "residual images of e-mail messages" sent via private e-mail accounts, policy's "admonishment to . . . employees that they would not enjoy privacy when using [their employer]'s computers or automated systems [wa]s clear and unambiguous") <wolfs2cents.files.wordpress.com/2007/03/usdc-sdny_long_v_marubeni2006usdistlex76594_19oct.pdf>

- *Nat'l Econ. Research Assocs. (NERA) v. Evans*, 21 Mass. L. Rep. 337, 2006 WL 2440008, 2006 Mass. Super. LEXIS 371 (**Mass. Super. Ct. 8/3/06**) ("if an employer wishes to read an employee's attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet, the employer must plainly communicate to the employee that: (1) all such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and (2) the company expressly reserves the right to retrieve those temporary files and read them.") <http://blog.mclane.com/wp-content/uploads/2011/09/National-Economic-Research-Associates-v.-Evans.pdf>

- *Curto v. Medical World Communics., Inc.*, 2006 WL 1318387, 99 Fair Empl. Prac. Cas. (BNA) 298 (**E.D.N.Y. 5/15/06**) (ex-employee had not waived privilege or work product immunity as to information recovered forensically from work-at-home laptop provided by employer) <www.internetlibrary.com/pdf/curto.pdf> (*distinguishing U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000))

- *Jiang, People v.*, 31 Cal. Rptr. 3d 227 (**Cal App. 6 Dist. 7/14/05**) (unpublished decision holding that attorney-client privilege covered documents on employer-issued laptop where employee had "made substantial efforts to protect the documents from disclosure by password-protecting them and segregating them in a clearly marked and designated folder") <http://caselaw.lp.findlaw.com/data2/californiastatecases/H026546.PDF>

I. Attorney-Client Privilege Opinions *(c't'd)*

- *Asia Global Crossing, Ltd., In re*, 322 B.R. 247, 251, 259 (**Bankr. S.D.N.Y. 3/21/05**) (no waiver of attorney-client privilege because "evidence [wa]s equivocal regarding the existence or notice of corporate policies") <internetlibrary.com/pdf/In-re-Asia-Global-Crossing-SD-NY-Bankruptcy.pdf>

- *McLaren v. Microsoft Corp.*, 1999 WL 339015 (**Tex. App. 5/28/99**) (no "reasonable expectation of privacy . . . where, at the time [Defendant-employer] accessed [Plaintiff-employee's] e-mail messages, [he] was on suspension pending an investigation into accusations . . . and had notified [Defendant] that some of the e-mails were relevant to the investigation[; a]ccordingly, the company's interest . . . would outweigh [Plaintiff's claimed privacy interest. . . .") <cyber.law.harvard.edu/privacy/McLaren_v_Microsoft.htm> (citing *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (**E.D. Pa. 1/23/96**) <loundy.com/CASES/Smyth_v_Pillsbury.html>)

II. Attorney-Client Privilege Articles

- Robert D. Brownstone, Sheeva J. Ghassemi & Soo Cho, *Privacy of Email and Text Messages – Case Law Sprinting to Catch Up to Modern Technology*, Privacy & Info. L. Rep., Bloomberg (3/1/11) <http://www.fenwick.com/fenwickdocuments/fenwick_west_brownstone_ghassemi-vanni_cho_article.pdf>

- Daniel J. McGravey and Amy C. Lachowicz, *Can Employers Review Electronic Messages?* Pa. Legal Intelligencer (9/14/10) <http://www.pietragallo.com/keep-informed.php?action=view&id=82>

- Diane Karpman, *Early client education can prevent big problems later*, ETHICS BYTE, Cal. B.J. (10/1/11) <http://www.calbarjournal.com/October2011/EthicsByte.aspx>

- Allison Shields, *Attorney-Client Confidentiality and Email*, Lawyerist (9/21/11) <http://lawyerist.com/attorney-client-confidentiality-email/>

- Marvin Goldstein and Mark Saloman, *New Jersey's High Court Ruling Reaffirms Employer's Right To Monitor and Restrict Computer Use -- Provides Guidance for Effective Internet Usage Policies*,15 Cyberspace Lawyer No. 4, at 1 (May 2010) <proskauer.com/publications/client-alert/new-jersey-high-court-reaffirms-employers-right-to-enforce/>

- Tresa Baldas, *Court Finds Personal E-Mail Privileged Even if Sent From Work*, Nat'l L.J. (12/14/09) <http://www.law.com/jsp/article.jsp?id=1202436284416>

- Anthony E. Davis, *Attorney-Client Privilege in Work E-Mails*, N.Y.L.J. (11/5/09) <http://www.law.com/jsp/law/article.jsp?id=1202435191463>

- Fernando M. Pinguelo and Andrew K. Taylor, *New Jersey Court Finds Waiver of Privilege in 'Loving' Way*, Fios (4/14/09) <http://Fios-Stengart.notlong.com>

- Philip L. Gordon and Kate H. Bally, *Web-Based E-mail Accounts Accessed At Work: Private Or Not? Look To The Handbook*, Littler Workplace Privacy Counsel (3/24/09) <http://Gordon-Bally-Littler.notlong.com>

- Michael F. Urbanski and Timothy E. Kirtner, *Employee Use of Company Computers – A Privilege Waiver Mine Field* , 57 Va. Lawyer 40 (2/1/09) <http://www.vsb.org/docs/valawyermagazine/vl0209_computers.pdf>

- Matthew J. Herrington and William T. Gordon, *Are You at Risk of Waiving the Attorney-Client Privilege by Using Your Employer's Computer Systems to Communicate With a Personal Attorney?*, 7 BNA PVSLR No. 18, at 685 (5/5/08) <http://www.steptoe.com/assets/attachments/3401.pdf>

Full Brownstone Bio & Bibliography at:

- Bio: <fenwick.com/bobbrownstone>

- Biblio: <fenwick.com/bobbrownstoneinsights> (articles, press quotes & speeches, oh my!)

APPENDIX D – Robert D. Brownstone – Social-Media Ethics – Lawyers, Jurors & Judges – Partial Bibliography (@ 2/8/13)

1. Lawyers

- **Exposing Client Confidences, Conflicts of Interest, etc.**
  - *Ethical Pitfalls*" – three-part series by Quarles & Brady (2011):
    - Part I <http://ediscovery.quarles.com/2011/06/articles/practice-tips/dr-seuss-cheese-and-social-media-ethical-pitfalls-impacting-attorneys-and-their-clients/>
    - Part II <http://ediscovery.quarles.com/2011/07/articles/practice-tips/dr-seuss-cheese-and-social-media-part-ii-ethical-pitfalls-pretexting-and-duties-of-candor/>
    - Part III <ediscovery.quarles.com/2011/10/articles/practice-tips/dr-seuss-cheese-and-social-media-part-iii-ethical-issues-involving-attorneys-and-their-judges/>
  - Brownstone & Grunfeld, *Ethical Attorney Advertising and Solicitation in the Social-Media Age*, Cal. State Bar (Sep. 15, 2011) <html.documation.com/cds/SBC2011/HTML%20Files/PDFs/014.pdf>
- **"Friend"-ing/Communicating w./ Witnesses, Represented Parties or Jurors**
  - ABCNY Formal Opinion 2012-2: Jury Research and Social Media <http://www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-formal-opinion-2012-02>
  - San Diego Cty. Bar Ass'n, *Legal Ethics Opinion 2011-2* (May 24, 2011) <http://www.sdcba.org/index.cfm?pg=LEC2011-2>
  - NYSBA Comm. On Prof'l Ethics, *Op. # 843* (Sep. 10, 2010) <http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&template=/CM/ContentDisplay.cfm&ContentID=55951>
  - Phila. Bar Ass'n, *Prof. Guidance Comm. Op. 2009-02* (Mar. 2009) <http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf>
- **Instructing Client to "Clean Up" Social-Media Pages While Discovery Pending**
  - *Lester v. Allied Concrete Co.*, Nos. CL.08-1S0 & CL09-223 **(Va. Cir. Ct. Charlottesville)**:
    - **Oct, 21, 2011 Order** in 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 132 (spoliation sanctions: $542,000 against Plaintiff's counsel; and $180,000 against Plaintiff) <.x1discovery.com/download/Lester_v_Allied_Concrete_Final_Order.pdf>
    - **Sep. 1, 2011 Opinion** (spoliation finding and damages remittitur where counsel had instructed client to "clean up" his social-media pages during lawsuit) <valawyersweekly.com/vlwblog/files/2011/09/Lester-Hogshire-order.pdf>
- **Investigations by Lawyers – Various Ethical Concerns**
  - Shane Witnov, *Investigating Facebook: The Ethics of Using Social Networking Websites In Legal Investigations*, 28 Santa Clara Computer & High Tech. J. # 1, at 79 (Nov. 2011) <digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1532&context=chtlj&sei-redir=1>

2. Jurors – Investigation/Research by and about . . . .

- Gibson & Capell, *Researching Jurors on the Internet—Ethical Implications*, NYSBA J. (Nov. 28, 2012) <nysba.org/AM/Template.cfm?Section=Home&Template=/CM/ContentDisplay.cfm&ContentID=126593>

- Bloomberg BNA Privacy & Security Law Report, *Kentucky Supreme Court Sets Guidelines For Using Social Media to Investigate Jurors*, 11 PVLR 1473 (10/1/12) <http://privacylaw.bna.com/pvrc/7057/split_display.adp?fedfid=28120155&vname=pvlrnotallissues&jd=a0d4u8h2q1&split=0> (subscription required)

- *Sluss v. Commonwealth*, 381 S.W.3d 215 (Ky. Sep. 20, 2012) (on appeal from murder conviction. remanding for post-conviction hearing as to potential juror bias where two jurors may have lied in voir dire when asked if they were on Facebook when in fact they may have been Facebook "friends" of a victim's mother) <http://caselaw.findlaw.com/ky-supreme-court/1612369.html>

- *Proposed Model Jury Instruction: The Use of Electronic Technology to Conduct Research on or Communicate about a Case*, Judicial Conference Committee on Court Administration and Case Management (June 2012) <http://www.uscourts.gov/uscourts/News/2012/jury-instructions.pdf>

- *Juror No. One v. Superior Court (Royster)*, 206 Cal. App. 4th 854, 142 Cal. Rptr. 3d 151, 153 (Cal. App. 3 Dist. May 31, 2012) (upholding "order requiring [j]uror . . . to execute [SCA] consent form . . . authorizing Facebook to release to the court for in camera review all items he posted during [criminal] trial") <http://www.courts.ca.gov/opinions/archive/C067309.PDF>

- *Vermont v. Abdi*, 2012 Vt. 4, 45 A.3d 29 (Jan. 26, 2012) (reversing and remanding for new trial in light of "juror's acquisition of information on the internet concerning Somali culture, a subject that played a significant role at trial") <http://info.libraries.vermont.gov/supct/current/op2010-255.html>

- *U.S. v, Juror No. One*, 866 F.Supp.2d 442 (E.D. Pa. Dec. 21, 2011) (finding juror guilty of contempt and sentencing her to $1,000 fine where "[a]fter being dismissed, [she had] disobeyed . . . orders and discussed via e-mail with other jurors her opinion on the Defendant's guilt") <gpo.gov/fdsys/pkg/USCOURTS-paed-2_10-cr-00703/pdf/USCOURTS-paed-2_10-cr-00703-5.pdf>

- *Dimas-Martinez v. Arkansas*, 2011 Ark. 515, 385 S.W.3d 238, 248-49 (Dec. 8, 2011) (fair trial right violated in part because one juror "disregarded the circuit court's instructions and tweeted about the case") <http://opinions.aoc.arkansas.gov/WebLink8/0/doc/252414/Electronic.aspx>

- Meghan Dunn, *Jurors' Use of Social Media During Trials and Deliberations; A Report to the Judicial Conference Committee on Court Administration and Case Management*, Federal Judicial Center (11/22/11) <fjc.gov/public/pdf.nsf/lookup/dunnjuror.pdf/$file/dunnjuror.pdf>

- Eva-Marie Ayala, *Tarrant County juror sentenced to community service for trying to 'friend' defendant on Facebook*, Ft. Worth Star-Telegram (Aug. 28, 2011) <http://www.tmcnet.com/usubmit/2011/08/29/5738118.htm>

- *Cal. A.B. 141* (signed by Gov. Brown Aug. 5, 2011) <www.leginfo.ca.gov/cgi-bin/postquery?bill_number=ab_141&sess=CUR&house=B&author=fuentes>

2. Jurors – Investigation/Research by and about . . . . *(c't'd)*

- NYCLA Comm. On Prof. Ethics, *Op. No. 743* (May 18, 2011) ("proper and ethical under [N.Y.] RPC 3.5 for a lawyer to undertake a pretrial search of a prospective juror's social networking site, provided that there is no contact or communication with the prospective juror and the lawyer does not seek to 'friend' jurors, subscribe to their Twitter accounts, send tweets to jurors or otherwise contact them") <www.nycla.org/siteFiles/Publications/Publications1450_0.pdf>
- Judge Linda F. Giles, *Does Justice Go Off Track When Jurors Go Online?* 55 Boston Bar. J. No. 2, at 7-9 (March 21, 2011) <www.bostonbar.org/pub/bbj/bbj_online/bbj1011/spring2011/bbj_spring2011.pdf#page=7>
- Brian Grow, *Internet v. Courts: Googling for the perfect juror*, Reuters Legal (Feb. 17, 2011) <reuters.com/article/2011/02/17/us-courts-voirdire-idUSTRE71G4VW20110217>

3. Judges

- Tenn. Judicial Ethics Committee Advisory Opinion No. 12-01 (Oct. 23, 2012) ("while judges may participate in social media, they must do so with caution and with the expectation that their use of the media likely will be scrutinized various reasons by others[;]judges must decide whether the benefit and utility of participating in social media justify the attendant risks.") <http://www.tncourts.gov/sites/default/files/docs/advisory_opinion_12-01.pdf >
- *Domville v. State*, 103 So.3d 184, 37 Fla. L. Weekly D2126 (Fla. App. 4 Dist. Sep. 5, 2012) (where presiding judge in criminal case had "friend"-ed assigned prosecutor on Facebook, reasonably prudent defendant would fear he could not receive a fair and impartial trial, so that Defendant's motion for disqualification granted; applying Fla. JEAC Op.2009–20 (Nov. 17, 2009) <http://www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2009/2009-20.html>) <http://www.4dca.org/opinions/Sept%202012/09-05-12/4D12-556.op.pdf>, *rehearing denied but question of great importance certified for Fla. Sup. Ct.*, --- So.3d ----, 2013 WL 163429 (Fla. App. 4 Dist. Jan. 16, 2013) <http://www.4dca.org/opinions/Jan%202013/01-16-13/4D12-556.rehg.pdf>
- Michael Crowell, *Judicial Ethics and Social Networking Sites*, UNC School of Government (revised August 2012) ("three states have concluded that a social network friendship is sufficiently likely to create the impression of special influence that it should be barred") <sog.unc.edu/sites/www.sog.unc.edu/files/Judges%20social%20networking%20Aug%2012.pdf>
- Md. Judicial Ethics Committee Op. Request No. 2012-07 (June 12, 2012) ("Judge Must Consider Limitations on Use of Social Networking Sites") <http://www.courts.state.md.us/ethics/opinions/2000s/2012-07.pdf>
- Mass. CJE Opinion No. 2011-6 (Dec. 28, 2011) <mass.gov/courts/sjc/cje/2011-6n.html>
- Okla. Judicial Ethics Advisory Panel, *Judicial Ethics Op. 2011-3* (July 6, 2011) <http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=464147>
- Ohio Sup. Ct., *Advisory Opinion: Judges May 'Friend' 'Tweet' if Proper Caution Exercised* (12/8/10) (linking to *Op. 2010-7* (Dec, 3, 2010) <sconet.state.oh.us/Boards/BOC/Advisory_Opinions/2010/Op_10-007.doc>)
- Kentucky Ethics Comm. Of the Ky. Judiciary, *FORMAL JUDICIAL ETHICS OPINION JE-119* (Jan. 20, 2010) <http://courts.ky.gov/commissionscommittees/JEC/JEC_Opinions/JE_119.pdf>

3. Judges *(c't'd)*

- Fla. Sup. Ct. Judicial Ethics Advisory Comm., *Op. No. 2009-20* (Nov. 17, 2009) <www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2009/2009-20.html>
- S.C. Advisory Comm. On Standards Of Judicial Conduct, *OP. NO. 17-2009 RE: Propriety of a magistrate judge being a member of a social networking site such as Facebook* (Oct. 2009) <www.judicial.state.sc.us/advisoryOpinions/displayadvopin.cfm?advOpinNo=17-2009>
- N.Y. Advisory Comm. on Judicial Ethics, *Op. 08-176* (Jan. 29, 2009) <http://www.courts.state.ny.us/ip/judicialethics/opinions/08-176.htm>
- N.C. Judicial Standards Comm'n, *Public Reprimand In re Terry*, Inquiry No. 08-234 (Apr. 1, 2009) <www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf
- Eugene Volokh, *May Judges Be Facebook "Friends" with Lawyers or Others Who Regularly Appear Before Them?* Volokh Conspiracy (Sep. 2, 2011) <http://volokh.com/2011/09/02/may-judges-be-facebook-friends-with-lawyers-or-others-who-regularly-appear-before-them/>
- Debra Cassens Weiss, *Ga. Judge Resigns After Questions Raised About Facebook Contacts*, ABA J. (1/7/10) (Ga. JQA investigation was pending) <abajournal.com/news/article/ga._judge_resigns_after_questions_raised_about_facebook_contacts/>

NELI ELB

APP. E

February/ March 2013

Vail & Las Vegas

The eWorkplace – Social-Media, Privacy & Info-Security Policies

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**
  - *Strange Things (Prospective) Employees Memorialize*
  - *Social-Media: Individual **and** Employer-Sponsored*
- **II. "MONITORING" ELECTRONIC ACTIVITIES**
  - *Some Justifications & Some Countervailing Concerns*
- **III. INVESTIGATIONS RE: EMPLOYEES / APPLICANTS**
  - *Following the Internet Trail*
- **IV. SEARCHING AND TRACKING VIRTUAL CONDUCT**
  - *?"Off-Duty"? (Web) Activities*
- **V. IMPLEMENTING LEGALLY-COMPLIANT AND DEFENSIBLE POLICIES *(time permitting)***
  - *Compliance Basics*

I. INTRO – Our Digital World

- **Modern differences:**
  - **"Frolic & detour" track-able**
    - ***See also* *Event data recorders installed in cars stirring controversy*, KTVU News (7/11/12); video report HERE**
  - **Ever-expanding universe of forums**
  - **Everyone's a publisher**
  - **MANY more ways to expose information**
  - **Personnel matters play out in public**

I(A). INTRO *(c't'd)* – Liability Risks & Data Leakage

- ***Unintentional*** **Loss or Theft of Sensitive Information**
  - **David Wallis, *Loose Lips Sink Company Trips*, NYT (5/3/12)**
  - ***Business Travel Security Holes*, Executive Counsel (June/July 2011)**
- ***Intentionally*** **Harmful Intentional Disclosures**
- ***Inadvertently*** **Harmful Intentional Disclosures ("Netiquette," Social-Media, etc.)**

I(A). INTRO *(c't'd)* – Our New World *(c't'd)*

- **Technology-Acceptable-Use Policy (TAUP) = No-Expectation- of-Privacy Policy (NoEEPP)**
  - **Many SAMPLES linked off Appendix A**
- **TWO KEYS TO DEFENSIBLE POLICIES:**
  - **POLICY CONTENTS**
  - **CONSISTENT ENFORCEMENT**

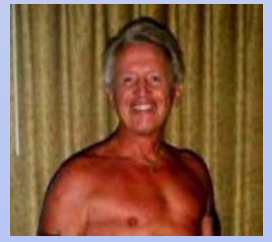
See detailed 3/18/13 article (incl. re: Harvard)

I. B. Strange Things People Memorialize

1. Liability Evidence – "Smoking Guns"

- **Ex-CIA Director David "All In" Petraeus**
  - **See articles at footnote 5 in Paper**

- **And semi-clad or unclad politicians . . . including EX-State Rep. in Fla. Peter Nehr**



  - **Jason Bartolone, *Shirtless Photos of State Rep. Peter Nehr Cause a Stir*, DunedinPatch (7/28/12)**
  - **Sunde Farquhar, *State Rep. District 65: Nehr Loses to Zimmermann*, Palm Harbor Patch (11/6/12)**

I(B). 2. Internet – Social-Media

- **Now, with Web 2.0/UGC, a bigger universe of web activities [some via F&W clients ☺]**

- **Social-media part of TAUP to address: 1) General Guidelines; 2) Company-Sponsored; & 3) Personal**

I(B)(1). Liability Evidence – Social-Media too

- ***Examples:***
  - **From sock-puppetry to "fascism" labeling**
    - **Whole Foods' John Mackey**
  - **Are 200,000 FB followers – or 1 Billion potential visitors ?! – a "select group" to the SEC?**
    - **Netflix' CEO Reed Hastings**
  - **Federal prosecutors' anonymous posts**
    - **U.S. Atty. For E.D. La. Jim Letten**

I(B)(2). Web 2.0 – Rewards . . . and . . .

- ***RISKS:***
  - **Every Post Can Last Forever**
    - **Search-ability**
    - **Capture-ability**
    - **Wayback Machine**
      - ***Now with 240,000,000,000 URLs*** **(1/9/13) (and ≈ 5 Petabytes of data)**
      - ***See also*** **Ainsworth, et al., *How Much of the Web Is Archived?* (1/8/13)**
    - **Tweets are especially persistent**
    - **Public Records archives**

I(B)(2). Social-Media / Web 2.0 *(c't'd)*

- ***RISKS*** *(c't'd)*:
  - **INCOMING! and . . . OUTBOUND!**
    - **U.S. DOJ, *INTERNET SOCIAL NETWORKING RISKS*, FBI Brochure (2/9/12)**
    - **Other FBI Brochures linked off this page**

I(B)(2). eDiscovery Decisions

- **Case-law keeps emerging**
  - **See Appendix B, esp.**
    - ***EEOC v. Simply Storage* AND**
    - ***E.E.O.C. v. Original Honeybaked Ham Co. of Georgia*, 2012 WL 5430974 (D. Colo. 11/7/12) (broad re: class of 20+) and . . .**
      - **. . . court-ordered questionnaire (1/9/13)**
  - ***"Not reasonably accessible"?***
    - ***Facebook – "Download Your Information"***
    - ***Twitter – "Your Twitter Archive" (in progress)***

I(B)(2). eDiscovery Decisions

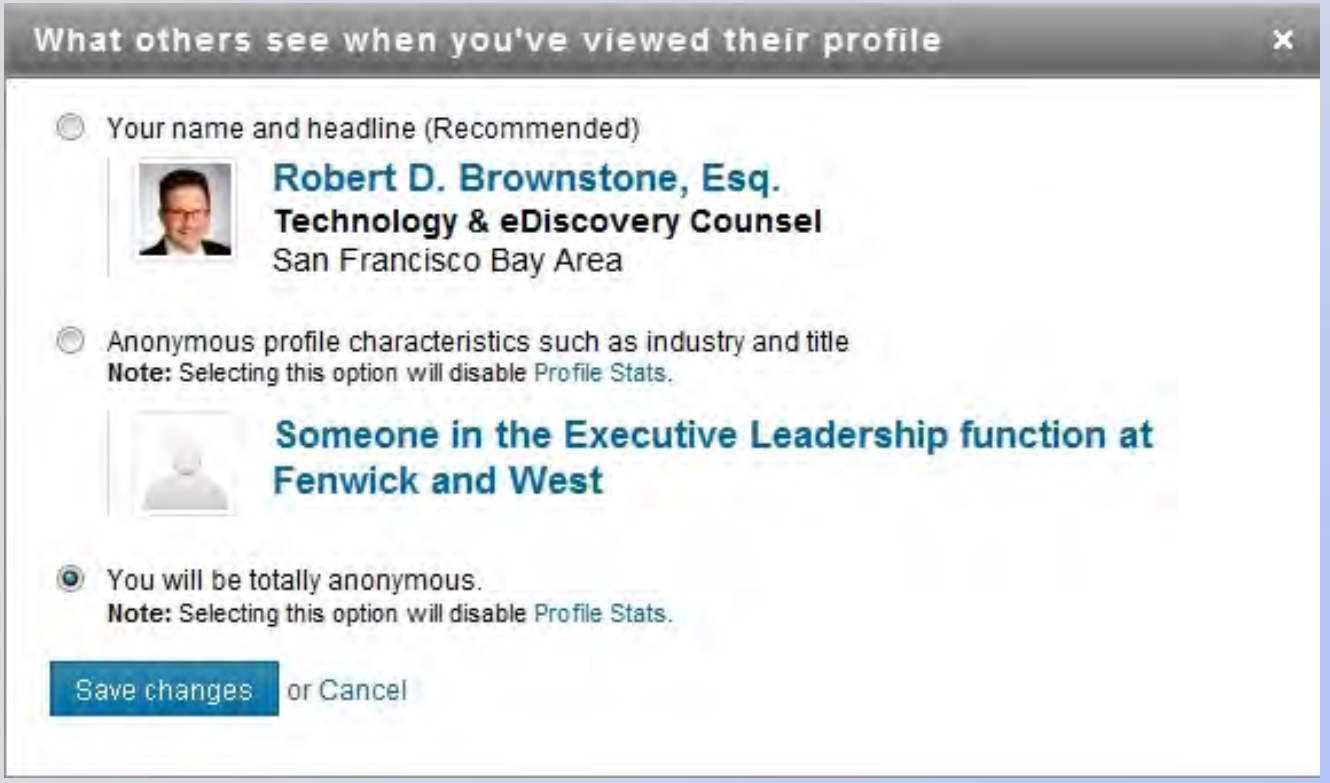
- **IF *company's* social-media data is pertinent, remember to preserve it. *See* this article.**
- **ALSO, aside from social-media, some landmark eDisco decisions in discrim. cases**
  - **Proportionality / preservation in *Pippins v. KPMG***
  - **Technology-assisted-review in *Moore v. Publicis***
    - ***See* p. 10 of Paper**

I(B)(2). Social-Media – Privacy?!

- **Recent developments:**
  - **Facebook:**
    - **Settings often change**
    - **"Frictionless" sharing**
  - **Ethics/sanctions developments re: lawyers, jurors & judges . . .**
    - **Appendix D**

II. Monitoring – Risk-Management Justifications

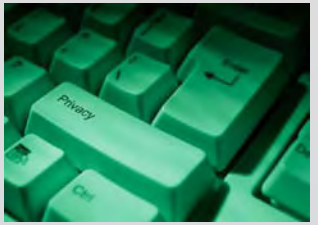
- **All of the above, plus, *e.g.*, unique LinkedIn ones:**
  - **Endorsements**
  - **Transparent profile searching?**



II. Monitoring – Risk-Management Justifications

- **REMEMBER 3 Types of Concerns**
  - **Track workers' activities, productivity & locations**
  - **Network security**
    - **Nov '11 FBI warnings to law firms**

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

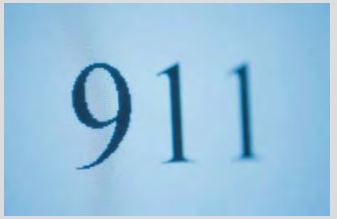


- **PLUS – Protecting Individuals' Personally Identifiable Information (PII):**
  - **States' notice-of-breach and other anti-identity-theft statutes linked here: <www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>**
- **PII incidents include: Battle Creek (Michigan); Baylor University and NASA ones. *See* pp. 4, 33-34 and 50 of Paper**
- ***See* my recent SHORT encryption video here**

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

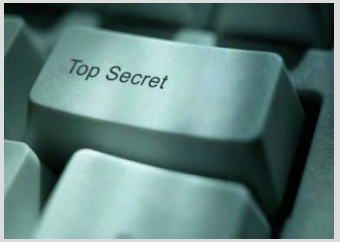
- **Protecting Individuals' Personally Identifiable Health Information (PHI):**
  - **HIPAA, as amended/expanded in Feb. '09 by HITECH part of ARRA stimulus package**
  - **Some states (Cal. & Ark.)**
  - **FTC's "Health Breach Notification Rule" [re: Personal Health Records (PHR) vendors]**
- **Recent Development**
  - **FINAL RULE re: "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under" HITECH, GINA, etc., HHS (1/17/13)**
- **See *What Do Employers Really Need to Know About the New HIPAA/HITECH Omnibus Final Rule?*, Littler (2/5/13)**

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



- **Loose Lips + Facebook Fingers =**
  - **Virginia Henschel, *Facebook Terminations: Friends Don't Let Friends Talk Smack About Their Job*, LexisNexis Applied Discovery Blog (4/12/10)**
  - **Fire Dep't EMS Supervisor/Lieutenant who "photographed a computer screen containing confidential and privileged information concerning a 911 caller's complaint of a gynecological emergency . . . And uploaded the image to. . . Facebook . . ., along with the caption '[c]an't make this up' "**
    - ***Palleschi v. Cassano*, --- N.Y.S.2d ----, 102 A.D. 3d 603 (N.Y. A.D. 1 Dept. 1/29/13) (upholding termination)**
  - **For more examples (nurses, EMT, etc.), click *here***

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



- **Stolen or Lost Laptop**
  - **Scott Graham, *Court to Decide if a Stolen Hard Drive Is Worth $4 Billion*, Recorder (1/25/13)**
  - **Cal. Confidentiality of Med. Info. Act at issue in *Sutter Medical Foundation cases* (Cal. App. 3 Dist.)**

II. Monitoring's Legality – Some Highlights

- **On whole, same rules applicable to employees' "reasonableness" arguments in Constitutional, statutory & common law**
- **REMEMBER Two Keys:**
  - **POLICY CONTENTS**
  - **CONSISTENT ENFORCEMENT**
- ***Quon v. Arch Wireless*, 130 S. Ct. 2619 (6/17/10)**
  - ***See* pp. 16-18 of Paper, incl. Top Ten Tips**

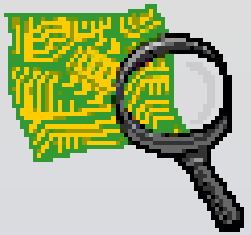
II. TAUP / NoEEPP *(c't'd)* – Privacy Expectations *(c't'd)*

- **BYOD a difficult issue. *See* pp. 18 & 40-41 in Paper. Are these alternatives viable?**
  - **Company-issued iPads?**
    - **Penny Crosman, *Banks to Workers: 'Bring-Your-Own-Device' Party Is Over*, American Banker (12/27/12)**
  - **Dual-identity phones?**
    - **Olga Kharif, *RIM leads 'bring your own device' market*, SF Chronicle (1/19/13)**
- ***See also* Intel's white papers on BYOD enablement and BYOD eDiscovery**

II. TAUP / NoEEPP *(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 an employee's attorney-client (a/c) privilege**
    - ***See* Appendix C and Paper at pp. 14-15.**
  - **illicitly obtaining password and accessing content in personal account or site**
    - ***See* pp. 15-16 & 40-41 in Paper (incl. *Sitton*)**

II. TAUP/NoEEPP *(c't'd)* – Privacy Expectations *(c't'd)*



- **As to latter exception (ECPA):**

compare:

- ***Shefts v. Petrakis***, **2012 WL 4049484 (C.D. Ill. 9/13/12) (Wiretap Act violated by spyware that covertly screen-captured received emails)**

with . . .

- ***Garcia v. City of Laredo***, **702 F.3d 788 (5th Cir. 12/12/12) (SCA not violated by unauthorized access to data stored on personal cell phone)**

II. CFAA Justification For Monitoring

- **CFAA**
  - **Two types of claims**
  - **MANY decisions since 2008**
  - **Two hurdles (case law split on each):**
    - **1) authorization / access**
      - **9th-Cir. / *Nosal (2012)* / *Brekka* (2009) vs. 7th-Cir. / Citrin (2006)**
    - **2) "loss"**
  - **See pp. 22-27 of Paper**

II. Another Concern – Union Activity

<pcworld.com/article/210402/careful_what_you_say_on_facebook_the_boss_is_watching.html>

<http://staffingtalk.com/nlrb-favors-facebook-firings/>

- **Lots of NLRB Activity (pp. 27-28 & 43-49 of Paper)**
  - **NEW: FOUR NLRB Decisions in Fall 2012**
  - ***GC Reports*, complaints, settlements & ALJ decisions (INCLUDING 5/30/12 Report)**
- **Drafting & Enforcement Tips? *See* my VERY short video here (no lying, no secrets . . .)**

II. Concerted Activity – The Future ? *(c't'd)*

- **Circuit court decision some day**
- **Will the 33 state PERB's follow suit?**
- **Is hitting the "like" button protected?**
  - **Patricia A. Dunn, *NLRB's Social Media Initiative: Not Much To "Like"*, Metropolitan Corp. Counsel (10/18/12)**
  - ***Compare Bland v. Roberts*, 857 F. Supp. 2d 599 (E.D. Va. Apr. 24, 2012) ("merely 'liking' a Facebook page is insufficient speech to merit constitutional protection"), *on appeal*, No. 12-1671 (4th Cir. 2012)**
    - ***See* p. 20 of Paper**

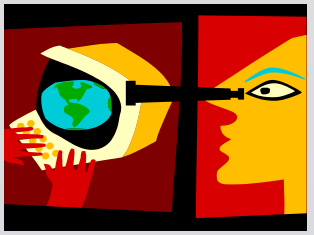
II. The Future Battlegrounds ? *(c't'd)*

- **In addition to the NLRA . . . ???**
- **ADA?!**
  - **Jon Hyman, *Internet-Use Disorder: The Newest Disability?* The Practical Employer (1/11/13)**
- **FMLA?!**
  - ***Jaszczyszyn* (leave abuse) and *Barnett* ("ding dong" FB message) – *see* pp. 38-39 of Paper**
  - **NEW! – *Lineberry v. Richards*, 2013 WL 438689, 20 Wage & Hour Cas.2d (BNA) 359 (E.D. Mich. 2/5/13) (leave abuse and dishonesty, like *Barnett*)**

III. Investigations and Background Checks

- ***Criminal history*** **(*e.g.*, Mass. CORI statutes)**
  - **As to Title VII disparate impact: EEOC Enforcement Guidance No. 915.002, *Consideration of Arrest and Conviction Records in Employment Decisions* (4/25/12)**
    - ***May consider convictions, not arrests***
    - ***Develop "targeted screen"***
    - ***Don't ask about convictions on job application UNLESS job-related & consistent w./ "business necessity"***
    - ***Perform individualized assessment***
      - ❖ ***See generally* this Fenwick summary**
- ***Credit report information*** **(FCRA & states' analogues)**
  - **Bans passed by CT, HI, IL, MD, OR, VT, WA and California (AB 22 effective 1/1/12)**

III. Investigations & Checks *(c't'd)*



- **What about asking applicant:**
  - **For Twitter *name* or Facebook URL to view public posts?**
  - **FB username AND password to view all content (incl. private)?**
  - **Forced shoulder-surfing?**
    - **See pp. 20-21 & 32-33 of Paper**
  - **College applicants – including athletes – of concern**

III. Investigations & Checks *(c't'd)*

- **State legislation:**
  - Maryland (eff. 10/1/12)
  - Michigan (eff. 12/28/12)
  - Illinois (eff. 1/1/13)
  - California (eff. 1/1/13)
  - 26 other states considering ban; see this NCSL compilation
- **Federal bills:**
  - Social Networking Online Protection Act (SNOPA): H.R. 5050 (4/27/12); and reintroduced (2/6/13)
  - *See also* Password Protection Act of 2012, H.R. 5684 (5/9/12)
- ***See generally*** this article **and** this one too

III. Applicants *(c't'd)* – Classifications

U.S. Equal Employment Opportunity Commission

From <eeoc.gov/policy/vii.html>:

Discrimination by Type

Laws, regulations and policy guidance, and also fact sheets, Q&As, best practices, and other information organized by basis of discrimination.

- Age
- Disability
- Equal Pay/Compensation
- Genetic Information
- National Origin
- Pregnancy
- Race/Color
- Religion
- Retaliation
- Sex
- Sexual Harassment

facebook

Information

Relationship Status:
Single

Birthday:
September 15, 1959

Information

Relationship Status:
Married to
[redacted]

Children:
[redacted]

Information

Political Views:
demo 4 insight

Religious Views:
buish or jewbu

III. Applicants *(c't'd)* – Classifications *(c't'd)*

- **State statutory protections too**
- **What could go wrong? Exs:**
  - **Loose lips or clumsy thumbs . . . .**
  - **"MODERN ASTRONOMY, THE BIBLE, AND CREATION" – *Gaskell v. Univ. of Ky.***

IV. "Off-Duty"? – Stupid Worker Tricks

- **Compare this one . . . .**

<mashable.com/2011/09/06/carol-bartz-fired/>

- ***See also*** **David Streitfeld, *Blunt E-Mail Raises Issues Over Firing at Yahoo*, N.Y. Times (Sep. 7, 2011)**

- **. . . with these:**
  - **Aimee Lee Ball, *Parting Is Such Sweet Revenge*, NYT (8/10/12)**
  - **Al Gore and Joel Hyatt, *Open letter to the viewers of Current* (3/30/12) (re: Keith Olbermann)**
  - **Christine Harper, *Goldman[,] Roiled by Op-Ed[,] Loses $2.2 Billion for Shareholders*, Bloomberg News (3/16/12)**
  - **James Temple, *Goldman Sachs is latest to hear wrath of ex-worker*, SFChron (3/16/12) (Google & Yahoo)**

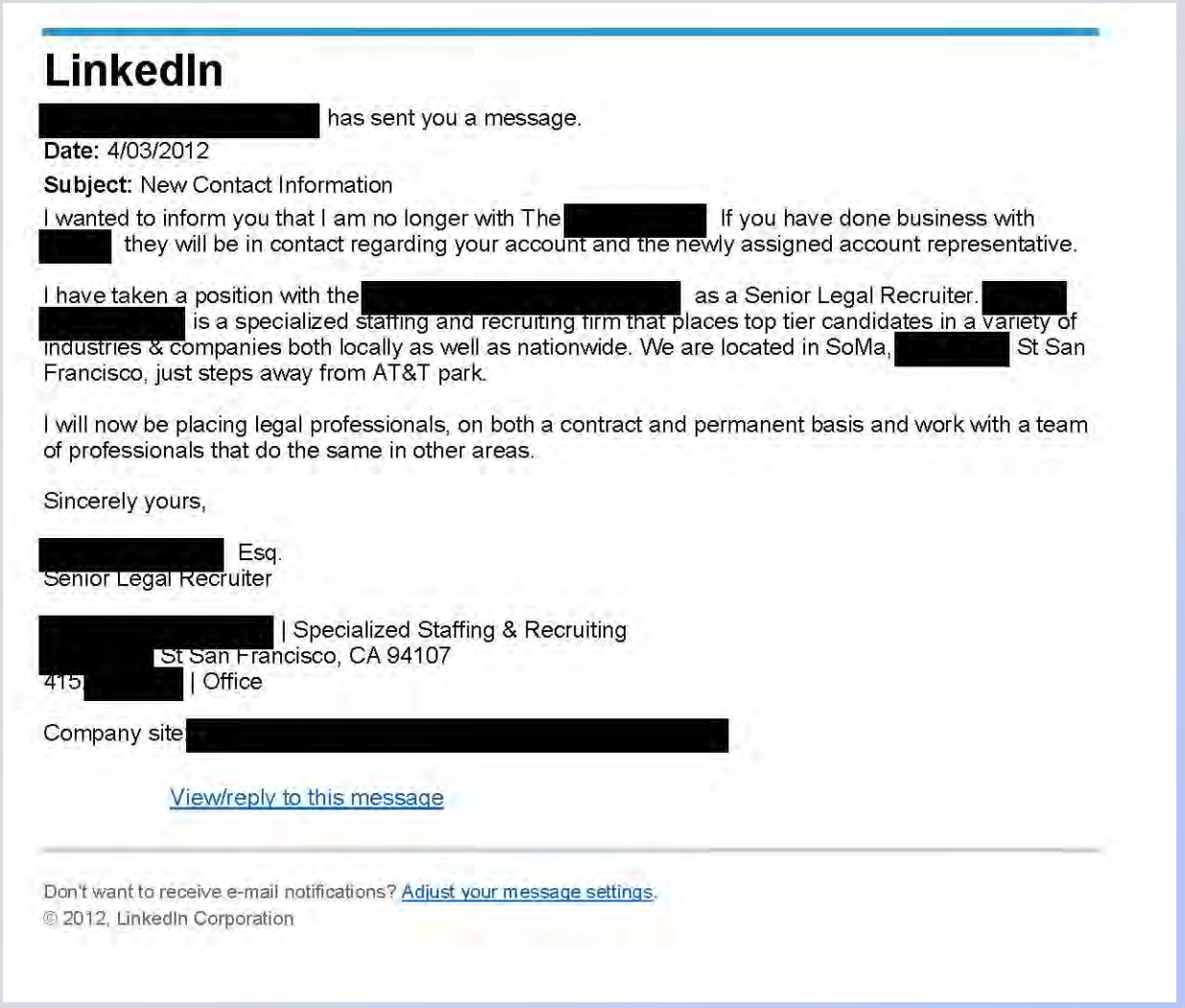
IV. "Off-Duty" Activities In Web Content *(c't'd)*

- **BUT there are always other new topics/questions . . .**
  - **What if boss or HR not "friend-ed" but receives a forward or a print-out from someone who is a friend? . . .**
    - ***See* interesting FMLA decision by 6th Cir. in *Jaszczyszyn* at pp. 38-39 of Paper**
    - ***See also* various examples in August 2011 and January 2012 NLRB GC Reports**

IV. Cutting Edge Issues re: Web Content *(c't'd)*

- **Who owns a Departed Employee's:**
  - **Twitter handle / account?**
  - **LinkedIn "connections"?**
- **Trade secret protection for employers for modern-day "eRolodexes" – either intra-company and / or on web?**
- ***See* p. 39 in Paper, including as to recent cases re: headhunters. . . . *See also* these 2 / 26 / 13 items: article and blog post**

IV. Cutting Edge Issues *(c't'd)*



LinkedIn

[redacted] has sent you a message.

Date: 4/03/2012

Subject: New Contact Information

I wanted to inform you that I am no longer with The [redacted] If you have done business with [redacted] they will be in contact regarding your account and the newly assigned account representative.

I have taken a position with the [redacted] as a Senior Legal Recruiter. [redacted] is a specialized staffing and recruiting firm that places top tier candidates in a variety of industries & companies both locally as well as nationwide. We are located in SoMa, [redacted] St San Francisco, just steps away from AT&T park.

I will now be placing legal professionals, on both a contract and permanent basis and work with a team of professionals that do the same in other areas.

Sincerely yours,

[redacted] Esq.
Senior Legal Recruiter

[redacted] | Specialized Staffing & Recruiting
[redacted] St San Francisco, CA 94107
415 [redacted] | Office

Company site [redacted]

View/reply to this message

Don't want to receive e-mail notifications? Adjust your message settings.
© 2012, LinkedIn Corporation

V. Compliance Basics

Let the Harmony Begin

TOSHIBA
Don't copy. Lead.®

- **KUMBAYA?!**

- **Clear, well-thought-out language on which multiple constituencies have weighed in . . .**
- **Compliance's "3 E's" = Establish / Educate / Enforce**
- **See Michael Rassmussen, *Policy Communication in a YouTube World*, Compliance Week (Sep. 25, 2012)**

Conclusion / Questions

Let's be careful out there . . .

- **Robert D. Brownstone (blog coming . . . !)**
  - **<fenwick.com/professionals/Pages/bobbrownstone_insights.aspx>**
  - **650.335.7912 or <rbrownstone@fenwick.com>**
  - **<twitter.com/ediscoveryguru>**
  - **<linkedin.com/pub/robert-d-brownstone-esq/0/a2/801>**
  - **<facebook.com/rbrownstone>**

- **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.