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

31st Annual Employment Law Briefing

March 2012 – Miami Beach, FL & San Diego, CA

eWorkplace Policies – Social-Media, Privacy & Internet-Security

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 teaches Electronic Discovery Law & Process classes at the University of San Francisco School (USF) of Law and Santa Clara University School of Law.

Bob is a member of four state bars, the NELI Advisory Board and the Board of Editors of ALM's *Internet Law & Strategy*. Bob is also the Immediate Past Chair of the Executive Committee of the State Bar of California's Law Practice Management and Technology (LPMT) Section.

For his full biography and bibliography, *see* <fenwick.com/attorneys/4.2.1.asp?aid=544>.

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

The eWorkplace – Technology-Use, Social-Media and Privacy Policies

Materials – TABLE OF CONTENTS

PAGE

PAPER

APPENDICES

TABLE OF CONTENTS

TABLE OF CONTENTS
(c't'd)

Page(s)

TABLE OF CONTENTS
(c't'd)

Page(s)

I. INTRODUCTION – THE MODERN LANDSCAPE[1]

A. Physical Conduct PLUS Digital Activity

Traditional concerns for employers have included: harassing or other discriminatory actions; other conduct leading to liability to third-parties; forbidden fraternizing; criminal activity; "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] In the era of data proliferation, employers have a heightened legitimate interest in protecting themselves.[3]

Given the mobility of electronic information, the stakes keep getting higher. Employees have access to, and are the gatekeepers of, trade secrets and other sensitive and confidential information. There are now many more ways that key information can be compromised, lost or stolen. The author typically parses the risks into three key categories, namely: 1) unintentional disclosures via loss, theft or hacking; 2) inadvertently harmful intentional disclosures; and 3) intentionally harmful intentional disclosures such as those on Wikileaks.[4]

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

Moreover, given the relatively desperate state of the economy the last few years, all indications are that employees are more likely to steal corporate information[5] and that organizations are even more worried about data

---

[1] The author especially thanks his current colleagues Sheeva J. Ghassemi-Vanni and Sebastian Kaplan as well as 2011 Summer Associate 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, Vic Schachter and Dan Ko Obuhanych – as well as his former colleagues John Fox, Juleen Konkel, Patrick Sherman and Shawna Swanson, Mary Wang and Soo Cho – for their contributions of prior content on which parts of this White Paper are based.

[2] *See* Robert D. Brownstone, *Workplace Privacy Policies* (Aug. 2009), at 1-3 (.pdf pp. 7-9) <fenwick.com/docstore/publications/EIM/eWorkplace_Policies_Materials_Public_Sector_EEO_8-28-09.pdf#page=7> (hereafter "Brownstone eWorkplace").

[3] For a discussion of employers' concerns about electronic media in the workplace, *see A Digital Crisis is Coming your Way. Are you Ready?* Forbes (Jul. 6, 2011) <http://blogs.forbes.com/forbesleadershipforum/2011/07/06/a-digital-crisis-is-coming-your-way-are-you-ready/>.

[4] In addition to the recent exposures of four decades of thousands of diplomatic cables reflected at Slide 26 of Appendix F, *see* Wikileaks, *Afghan War Diary 2004-2010* (six years of 92,000 of reports) <http://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010>; Ellen Nakashima and Joby Warrick, *Wikileaks takes new approach in latest release of documents*, Wash. Post (July 26, 2010) <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/26/AR2010072602084_pf.html>; N.Y. Times, *Piecing Together the Reports, and Deciding What to Publish* (July 25, 2010) <www.nytimes.com/2010/07/26/world/26editors-note.html>; Leila Fadel, *Army intelligence analyst charged in Wikileaks case*, Wash. Post (July 7, 2010) (video showing civilians killed in Iraq air strike) <washingtonpost.com/wp-dyn/content/article/2010/07/06/AR2010070602330_pf.html>; Kevin Poulsen and Kim Zetter, *State Department Anxious About Possible Leak of Cables to Wikileaks*, Wired (June 8, 2010) <wired.com/threatlevel/2010/06/state-department-anxious/>; Poulsen and Zetter, *U.S. Intelligence Analyst Arrested in Wikileaks Video Probe*, Wired (June 6, 2010) <wired.com/threatlevel/2010/06/leak/>.

[5] Information Management, *37% of [UK] Employees Would Sell Data*, Info. Mgmt., at 18 (Sep./Oct. 2009).

leakage, whether intentional[6] or unintentional. Thus, monitoring of employees' digital activity seems to have increased to an all-time high.[7]

Employers and their employees must carefully guard information belonging to or concerning: the organization itself; related companies; and even adversarial entities. Yet another constituency at risk for data leakage is the group of employees. During 2009, two highly publicized incidents ostensibly involved the loss of personally identifiable information ("PII") as to 97,000[8] and 29,000[9] co-workers, respectively. In the latter situation, the theft occurred while the data was in the possession of the employees' labor union rather than of the employer itself.[10]

Employers face an increasingly challenging environment with new and sometimes conflicting responsibilities to employees. Millions of employees' electronic activities can be under ongoing surveillance as to content, length, attachments, time spent and keystrokes.[11] Next-generation capabilities now include: measures such as: biometrics for security, timekeeping and attendance; recording employees' voice-based

---

[6] Good starting points for learning about some of the many ways technology tools can be leveraged to try to protect against trade secret leakage, see these Wikipedia entries on: *Information Rights Management* <http://en.wikipedia.org/wiki/Information_Rights_Management>; and *Digital Rights Management* <http://en.wikipedia.org/wiki/Digital_rights_management>.

[7] Proofpoint, Inc., *Outbound Email and Data Loss Prevention in Today's Enterprise, 2009* (Aug. 7, 2009) <proofpoint.com/downloads/Proofpoint-Outbound-Email-and-Data-Loss-Prevention-2009.pdf>. Among the articles about the Proofpoint study are Tresa Baldas, *New Hires to Monitor Outbound E-Mail*, Nat'l L.J. (Sep. 30, 2009) <law.com/jsp/cc/PubArticleCC.jsp?id=1202434171378>; Christine Mumford, *Lawyers Urge Caution Amid Increasing Incidence of Workplace Electronic Monitoring*, 8 PVLR 1295 (BNA Sep. 7, 2009), available by subscription at <news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=14923941&vname=pvlrnotallissues&fn=14923941&jd=a0b9t5e3k9&split=0>.

[8] *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. Dec. 14, 2010) ("Plaintiffs-Appellants . . . sufficiently alleged an injury-in-fact for purposes of Article III standing" where they "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data") ("*Krottner I")* <ca9.uscourts.gov/datastore/opinions/2010/12/14/09-35823.pdf> ; *but see Krottner v. Starbucks Corp.*, 2010 WL 5185487, 31 IER Cases 1123 (9th Cir. Dec. 14, 2010) ("*Krottner II")* <ca9.uscourts.gov/datastore/memoranda/2010/12/14/09-35823.pdf>. *See also* Class Action Complaint, *Krottner v. Starbucks Corp.*, No. 09-CV-00216-CMP (W.D. Wash. Feb. 19, 2009) (alleging that, in late October 2008, laptop containing PII – names, addresses and Social Security numbers – was stolen from a corporate facility, resulting in some apparent identity thefts as well as risk of many more) <https://ecf.wawd.uscourts.gov/doc1/19703090338>; Fenwick & West, *Starbucks Sued For Failing To Safeguard Employee Information*, Emp. Brief (Mar. 12, 2009) ("complaint also alleged that Starbucks had previously [-- in 2006 --] misplaced another laptop which contained the personal information of 60,000 employees") <fenwick.com/publications/6.5.4.asp?mid=44&WT.mc_id=EB_031209>.

[9] *Kaiser Permanente Comments on Northern California Employee Information Breach*, Our Point of View (Feb. 27, 2009) ("law enforcement had seized a computer file containing Kaiser Permanente Northern California employee information found in possession of a suspect who was arrested") <http://xnet.kp.org/newscenter/pointofview/2009/020609breach.html>.

[10] *Id.* ("[b]ased on forensic evidence and documentation uncovered by law enforcement, it appears that the information was taken in July 2007 from the offices of United Healthcare Workers (UHW) . . . ."). *See also* Elinor Mills, *Kaiser: Worker data breached, identity fraud reported* , cnet (Feb. 27, 2009) (Kaiser "offer[ed] one year of free credit monitoring for anyone who is affected"). <news.cnet.com/8301-1009_3-10158957-83.html>.

[11] Brownstone eWorkplace, supra note 2, at 3 (.pdf p. 9) <http://White-Paper-8-09-at-9.notlong.com>.

and data-based conversations;[12] and virtual call-center software that can monitor workloads and productivity of work-at-home independent contractors.[13]

While technological developments provide employers with new tools to monitor employees' electronic activities in the workplace, they also create new risks of liability for invasion of privacy, as well as potentially lowered morale and mistrust by employees.

In spite of these risks, employers have many legitimate reasons to monitor their employees' electronic communications in the workplace.[14] 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.

B. Strange Things People Memorialize – Overview of Liability Risks

Throughout this decade, e-mail messages – and other types of digital gaffes – have become more and more pivotal in litigation and in the court of public opinion. Recent examples of well-known figures laid low include: Rupert Murdoch's and some of Scotland Yard's highest-ranking police officers in the News of the World phone-hacking scandal;[15] and Anthony Weiner in the junk-mail tweets situation.

---

[12] Renai LeMay, *RIM changes tune on employee calls*, cnet news (Mar. 18, 2009) <http://news.cnet.com/8301-1035_3-10199076-94.html>.

[13] Damon Darlin, *PING: Software That Monitors Your Work, Wherever You Are*, N.Y. Times (Apr. 12, 2009) <http://www.nytimes.com/2009/04/12/business/12ping.htm>.

[14] For some startling actual numbers (not a survey), see the data available at Palo Alto Networks (PAN), *Application Usage and Risk Report* (6th Ed. Oct. 2010) <www.paloaltonetworks.com/researchcenter/reports/>. Some of that data is also summarized at Slide 12 of Appendix F to this White Paper.

[15] Jo Becker And Don Van Natta Jr., *2007 Letter Clearing a Tabloid Comes Under Scrutiny*, N.Y. Times (July 29, 2011) <http://www.nytimes.com/2011/07/30/world/europe/30letter.html>; David Leigh and Nick Davies, *The 'For Neville' email: two words that could bring down an empire*, Guardian (July 22, 2011) <http://www.guardian.co.uk/media/2011/jul/22/for-neville-email-empire>; Jillian Rayfield, *Two Ex-News Of The World Employees Claim James Murdoch Misled Parliament*, TPM (July 21, 2011) <http://tpmmuckraker.talkingpointsmemo.com/2011/07/two_ex-news_of_the_world_employees_claim_james_mur.php>.

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.[16] 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. In the past year, this scenario has been exemplified by: the HBGary campaign against Wikileaks, the "Anonymous" hacker(s) and a Salon reporter;[17] and Facebook's admitted attempts to malign Google.[18]

Knowledge of, and indifference to, inappropriate conduct are often memorialized as well. For instance, a JP Morgan employee wrote in an email that he had been told that "there [wa]s a well-known cloud over the head of Madoff and that his returns [we]re speculated." That email and others were cited in a $6.4 billion complaint alleging that JPMorgan was complicit in Madoff's Ponzi scheme.[19]

---

[16] ***Business***; Matthew Day and Ray Henry, *Documents Reveal BP's Missteps Before Blowout*, MSNBC (June 14, 2010) <msnbc.msn.com/id/37695879>; Frank Ahrens, *Former Toyota Exec Said in E-mail: 'We need to come clean,"* The Washington Post (April 7, 2010) <voices.washingtonpost.com/economy-watch/2010/04/ap_former_toyota_exec_said_in.html>. ***National politics***: In addition to the Christopher Lee and Anthony Weiner articles cited at Slides 9-10 of Appendix F, *see* Eric Lipton and John M. Broder, *E-Mail Shows Senior Energy Official Pushed Solyndra Loan*, N.Y. Times (Oct. 7, 2011) <nytimes.com/2011/10/08/us/politics/e-mail-shows-senior-energy-official-pushed-solyndra-loan.html >; Matthew L. Wald, *E-Mails Suggest White House Weighed a 2nd Solyndra Loan Worth Almost Half a Billion Dollars*, N.Y. Times (Oct. 6, 2011) <nytimes.com/2011/10/06/us/politics/2nd-us-loan-to-solyndra-said-to-have-been-considered.html>; Charlie Savage, *E-Mails Show Three Officials Were Informed of Gun Inquiry*, N.Y. Times (Sep. 2, 2011) <http://www.nytimes.com/2011/09/03/us/03guns.html> ; Gail Collins, *Semi-Naked Came the Congressman* The New York Times (Feb. 12, 2011) <nytimes.com/2011/02/12/opinion/12collins.html>. ***Local politics***: Brownstone eWorkplace, supra note 2, at 4-6 (.pdf pp. 10-12) <http://White-Paper-8-09-at-10.notlong.com>. *See also* these articles, which supplement Appendix H of that White Paper: Tresa Baldas, *Judge says enough, sends ex-Detroit mayor back to prison*, Nat'l L.J. (May 25, 2010) <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202458757140>; Tresa Baldas, *Disciplinary panels find misconduct by two lawyers in Detroit text-messaging scandal*, Nat'l L.J. (Mar. 2, 2010) <law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202445363577>; Tresa Baldas, *Former Detroit mayor staves off arrest over missed payment — for now*, Nat'l L. J. (Feb. 25, 2010) <law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202444699628> ; Tresa Baldas, *Ex-Detroit mayor argues he can't make restitution because 'burgers and beer' aren't enough*, Nat'l L. J. (Feb. 24, 2010) <law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202444506523>; Tresa Baldas, *Former Detroit Mayor Loses Case Against Lawyer Who Leaked Scandalous Text Messages*, Nat'l L. J. (Feb. 1, 2010) <law.com/jsp/article.jsp?id=1202439674972>; Tresa Baldas, *Five Lawyers Involved in Detroit Text Message Scandal Charged With Professional Misconduct*, Nat'l L. J. (May 21, 2009) <law.com/jsp/article.jsp?id=1202430879282>.

[17] Hackers posted an internet security company's internal emails online, reportedly revealing correspondence with a law firm seeking help to undermine the company's adversaries and critics. *See* Glenn Greenwald, *More facts emerge about the leaked smear campaign*, Salon (Feb. 15, 2011) <http://www.salon.com/news/opinion/glenn_greenwald/2011/02/15/palantir>; David Ingram, *Complaint Accuses Hunton & Williams of Dirty Tricks*, Nat'l L. J. (Feb. 25, 2011) <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202483172932>. For background about HBGary and Anonymous, *see generally* John Bullock, *HBGary v. Anonymous: How it Happened*, Geekti.me (Mar. 2011) <http://geekti.me/wp/2011/03/hbgary-vs-anonymous-how-it-happened>.

[18] Facebook admitted to being behind a campaign against Google when emails leaked. Amy Lee, *Google Smear Campaign Leaves Facebook Looking Desperate,* Huffington Post (updated May 25, 2011) <http://www.huffingtonpost.com/2011/05/12/facebook-google-pr_n_861165.html>. *See* the emails leaked at <http://pastebin.com/zaeTeJeJ>. *See also* Kashmir Hill, *Facebook Admits to Being Behind Smear Campaign Against Google* (May 12, 2011) <http://blogs.forbes.com/kashmirhill/2011/05/12/facebook-admits-being-behind-smear-campaign-against-google/>.

[19] *See* CBS News, *Lawyers: JPMorgan Complicit in Madoff's Fraud* (Feb. 4, 2011) <http://www.cbsnews.com/stories/2011/02/04/business/main7316833.shtml>; David Gardner, *Top Wall St. Bank "Suspected Bernie Madoff 18 Months Before his Scam was Revealed – But Kept Doing Business with him,* Daily Mail (updated Feb. 4, 2011) <http://www.dailymail.co.uk/news/article-1353476/JP-Morgan-Chase-suspected-Bernie-Madoff-18-months-scam-revealed--kept-doing-business-him.html>.

In harassment or discrimination cases, one or two explicit messages can bolster other evidence of hostile environment or discrimination.[20] For example, consider this gem that, in 2009, led to a huge verdict in an age discrimination case against Kmart: "Hawkins is 64 yrs old with 20 yrs with km. I think I can get him to retire. Let me work on him."[21]

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.[22]

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.

Furthermore, web activity can cause serious security breaches for employers. In the public sector, in 2009, the mayor of Battle Creek Michigan posted on the web a document containing personally identifiable information as to 65 city employees, including Social Security numbers for six of them.[23] As to the private sector, a recent study found that 12% of data loss at U.S. companies is from web-based activities.[24]

Other lurking potential dangers include phishing and/or whaling schemes as well as e-mail messages containing malware and/or links to malicious websites.[25] Employees' use of social networking sites increases employers' vulnerability to malware.[26]

---

[20] Brownstone eWorkplace, supra note 2, at 4-6 (.pdf pp. 10-12) <http://White-Paper-8-09-at-10.notlong.com>. *See also* The HR Specialist, *Warn Bosses: E-mail is Smoking Gun Evidence*, Business Management Daily (Mar. 26, 2011) <http://www.businessmanagementdaily.com/articles/25210/1/Warn-bosses-E-mail-is-smoking-gun-evidence/Page1.html#> (discussing *Salisbury v. City of Pittsburgh*, No. 08-CV-0125 (W.D. Pa, filed Jan. 28, 2008), a now-settled case that survived summary judgment, where Plaintiff had alleged that HR emails show prejudice against her because of her past involvement in protected activity and that managers had a racially biased view of financial problems). The *Salisbury* eDocket is available on PACER at <https://ecf.pawd.uscourts.gov/cgi-bin/DktRpt.pl?689484467777152-L_452_0-1>.

[21] Jason W. Armstrong, *Mystery E-Mail Leads Del Mar Lawyers to Huge Verdict, New Niche*, Daily J. (Aug. 27, 2009) ("e-mail triggered testimony that helped persuade a Riverside jury . . . to award . . . nearly $1 million in compensatory damages and $25 million in punitive damages"), available by subscription at <http://www.callawyer.com/story.cfm?eid=903980&evid=1>.

[22] *See generally* the lists at pp. 15 and 17 of <nascio.org/publications/documents/NASCIO-SocialMedia.pdf>.

[23] ComputerWeekly.com, *Top 10 Twitter marketing blunders in photos, Mayor Mark Behnke* (July 2, 2009) <http://www.computerweekly.com/galleries/236700-10/Mayor-Mark-Behnke-Top-10-Twitter-marketing-blunders.htm>; Newkirk, Barrett, *Battle Creek mayor accidentally tweets employee Social Security numbers*, Battle Creek Enquirer (June 24, 2009) <http://m.freep.com/news.jsp?key=481472>; Macaluso, Nora, *Mayor's 'Tweet' Accidentally Posts Personal Employee Data on Twitter*, BNA PSLR (June 29, 2009), available by subscription at <http://PSLR-6-29-09.notlong.com>.

[24] See Nigel Kendall, *Privacy Matters*, Wall St. J. (June 29, 2011) <online.wsj.com/article/SB10001424052702303714704576382892280173266.html?mod=googlenews_wsj>.

[25] *See* Brownstone eWorkplace, supra note 2, at 8 (.pdf p. 14) <http://White-Paper-8-09-at-14.notlong.com>.

b. Posts on Chatrooms, Blogs, Wikis, Social Networking Sites, Twitter, 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, online bulletin boards, Web surfing, and "blogs,"[27] the past few years have seen extraordinarily prolific use of smartphones[28] and social-networking.[29] These new ways of communicating introduce new challenges for employers. On the heels of a scandal involving explicit photographs Brett Favre sent via cellphone to a co-worker on the New York Jets professional football team, NFL Spokesman Greg Aiello noted that "[i]t's a totally different world with the Internet. … Information and videos that never once existed are the new reality and the new news."[30]

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.

Day-to-day issues include employees' posts that: criticize the employer;[31] reflect negatively on the employer;[32] and leave the employer open to vicarious liability.[33] In addition, private sector employees' posts

---

[26] Caroline McCarthy, *Study: Fifth of Facebook Users Exposed to Malware*, CNET (Nov. 22, 2010)<http://news.cnet.com/8301-13577_3-20023626-36.html?tag=mncol;1n>; *see also* Emily Steel and Geoffrey A. Fowler, *Facebook in Privacy Breach*, The Wall Street Journal (Oct. 18, 2010) <http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html>.

[27] Brownstone eWorkplace, supra note 2, at 8-13 (.pdf pp. 14-19) (including sock-puppeting) <http://White-Paper-8-09-at-14.notlong.com>. As to sock-puppeting, *see also* Chelsea Peters, *Whole Foods, Unwholesome Practices: Will Sock Puppeteers be Held Accountable for Pseudonymous Web Postings?*, 5 Shidler J.L. Com. & Tech. 4 (Sep. 23, 2008) <lctjournal.washington.edu/Vol5/A04Peters.html>; *SEC v. Curshen*, 2010 WL 1444910 (10th Cir. Apr. 13, 2010) <ca10.uscourts.gov/opinions/09/09-1196.pdf>; David Baker, *Another Ex: Embattled PG&E SmartMeter Executive Resigns*, SFGate (Nov. 11, 2010) <http://articles.sfgate.com/2010-11-11/business/24826008_1_smartmeter-program-discussion-group-resignation> (SmartMeter executive resigned after using an alias in an online discussion group of SmartMeter opponents).

[28] Int'l Data Group, *IDG Global Survey Shows Smartphone Use Growing Rapidly with Regional Differences*, Press Release (July 11, 2011) <http://www.marketwatch.com/story/idg-global-survey-shows-smartphone-use-growing-rapidly-with-regional-differences-2011-07-11?reflink=MW_news_stmp>.

[29] While it took television 13 years and the Internet four years to reach 50 million users, Facebook reached over 200 million users in less than a year. Erik Qualman, *Socialnomics: How Social Media Transforms the Way We Live and Do Business*, available at <http://www.socialnomics.net/the-book/>. *Facebook inches past Google for Web users' minutes*, AP (Sep. 10, 2010) ("surpassed . . . all of Google Inc.'s sites combined, including YouTube, . . . Gmail [and] Google news . . . ") <http://news.yahoo.com/s/ap/20100910/ap_on_bi_ge/us_facebook_catching_google/print>. For more books on the power of social-media, *see* Francois Gossieaux & Ed Moran, *The Hyper-Social Organization* (2010), purchasable at links provided at <human1.com/the-hyper-social-organization>; Don Tapscott & Anthony D. Williams, MACROWIKINOMICS (2010), purchasable at links provided at <http://www.macrowikinomics.com/order> (follow-up to WIKINOMICS book (2007) <http://www.wikinomics.com/book/>).

[30] Richard Sandomir, *N.F.L. Is Compelled to React*, The New York Times (Oct. 11, 2010) <nytimes.com/2010/10/12/sports/football/12sandomir.html?pagewanted=print>. *See also* Brian Hall, *Lawsuit Against Favre Not a "Text"book Case of Sexual Harassment,* Employer Law Report (Jan. 5, 2011) <http://www.employerlawreport.com/2011/01/articles/eeo/lawsuit-against-favre-not-a-textbook-case-of-sexual-harassment/#axzz1RkXNbAiK>.

[31] *See* Section V(B)(3) for a discussion of various proceedings in which the NLRB has assessed whether an employer committed an unfair criticism of employers.

may also violate: Federal antitrust laws;[34] Federal securities laws;[35] FINRA broker standards;[36] FTC online-advertising guidelines as to endorsements and testimonials;[37] and/or Federal Drug Administration regulations as to prescription-drug advertising.[38]

The Web 2.0[39] world of user-generated content (UGC), including employees' respective individual home pages on social networking sites and ill-advised tweets on Twitter[40] have begun to extend traditional

---

[32] Stuart Elliott, *When the Marketing Reach of Social Media Backfires*, The New York Times (March 15, 2011) <http://www.nytimes.com/2011/03/16/business/media/16adco.html> (discussing Gilbert Gottfried's dismissal as voice of squawking AFLAC spokes-duck after a controversial tweet); Kashmir Hill, *Tweets That Will Get You Fired*, Forbes (Mar. 17, 2011) <http://blogs.forbes.com/kashmirhill/2011/03/17/tweets-that-will-get-you-fired/> (discussing recent Twitter missteps and providing recommendations for employers).

[33] In *Spooner v. Associated Press*, filed on March 11, 2011 in federal court in Minnesota, an NBA referee sued the Associated Press and one if its sports writers for defamation. The writer's tweet allegedly implied that the referee had engaged in game-fixing: "Ref Bill Spooner told Rambis he'd 'get it back' after a bad call. Then he made an even worse call on Rockets. That's NBA officiating folks." <http://dockets.justia.com/docket/minnesota/mndce/0:2011cv00642/119133/>.

[34] *See* footnote 27 supra

[35] *Id*.

[36] *FINRA Regulatory Notice 11-39– Social Media Websites and the Use of Personal Devices for Business Communications* (Aug. 17, 2011) <finra.org/industry/regulation/notices/2011/p124187> (linking to .pdf of Guidance itself); *FINRA Regulatory Notice 10-06 –Social Media Web Sites: Guidance on Blogs and Social Networking Web Sites* (Jan. 25, 2010) <finra.org/Newsroom/NewsReleases/2010/P120780> (linking to .pdf of Guidance itself). *See also* Danielle Kucera, *Tweeting Rules May Leave Brokers With Little to Say to Clients*, Bloomberg (Dec. 3, 2010) <http://pennystockdd.com/stock-news/tweeting-rules-may-leave-brokers-with-little-to-say-to-clients/>.

[37] *FTC Pursues Online Endorsements by Undisclosed Insiders*, Fenwick & West Litigation Alert (September 2, 2010) <fenwick.com/docstore/Publications/Litigation/Litigation_Alert_09-02-10.pdf>.

[38] *See* Mandy Jackson, *Biotechs Reach for Customers on Social Media Without FDA Guidelines*, Daily Journal (June 8, 2011) <http://www.gordonrees.com/documents/ARTICLE%20-%20George%20NG%20Daily%20Journal%2006082011.pdf>; Doug Wood, *FDA Prescription for Online Medical Confusion*, Corporate Counsel (Mar. 29, 2011) <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202488382153>; Greenberg & Bederman, *FDA Monitors Drug Company on Social Marketing Sites,* Maryland Injury and Disability Law (Sept. 3, 2010) <http://www.mdinjurydisabilitylaw.com/2010/09/articles/prod-liab/fda-monitors-drug-company-on-social-marketing-sites/print.html>. For an example of an FDA dispute about social media, *see* John Mack, *Implications of FDA's Warning Letter to Novartis Regarding Facebook Share Widget*, Pharma Marketing Blog (Aug. 5, 2010) <http://pharmamkting.blogspot.com/2010/08/implications-of-fdas-warning-letter-to.html>; "Facebook Share" warning letter from the FDA to Novartis (July 29, 2010) <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCcompanies/UCM221325.pdf>.

[39] "Web 2.0 refers to the second generation of the Web, which enables people with no specialized technical knowledge to create their own websites, to self-publish, create and upload audio and video files, share photos and information and complete a variety of other tasks." Linda Young, *A social media glossary*, Capilano Univ. Active CMS (July 2008) <capilanou.ca/help/login-page/active-cms/glossary.html#Web%202.0>.

legal concepts into new contexts.[41] 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.

Anyone 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.[42] Social media information is increasingly archived, making it, at times, available even when it has been removed by the original author.[43] This search-ability[44] and persistence are compounded by general ignorance of, or failure to keep abreast of

---

[40] To learn more about tweeting on Twitter and/or more generally engaging in online social networking, *see* Davia Temin, *The 10 'Don't of Corporate Social Media*, Forbes (Aug. 4, 2011) <http://www.forbes.com/sites/daviatemin/2011/08/04/the-10-donts-of-corporate-social-media/>; Tony Bradley, *How to Use Twitter Like a Pro*, PCWorld (Jun. 12, 2011) <http://www.pcworld.com/businesscenter/article/230066/how_to_use_twitter_like_a_pro.html>; Verne Kopytoff, *Sharing your life online: How much is too much?* SF Chronicle (Apr. 27, 2009) <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/27/MN05174FPA.DTL&type=printable>; Maureen Dowd, *To Tweet or Not to Tweet*, N.Y. Times (Apr. 22, 2009) <http://www.nytimes.com/2009/04/22/opinion/22dowd.html?pagewanted=print>; Morgan W. Estes and Jim Calloway, *To Tweet, or Not To Tweet?*, Okla. Bar Ass'n (Apr. 7, 2009) <http://www.okbar.org/news/front/2009/04/to-tweet-or-not-to-tweet.htm>; Miral Fahmy, *Facebook, YouTube at work make better employees: study*, Reuters (Apr. 2, 2009) <http://www.reuters.com/articlePrint?articleId=USTRE5313G220090402>; Gina F. Rubel, *Is Twitter a valuable networking tool or just for the birds?* The Legal Intelligencer (Mar. 18, 2009) <law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202429165569>; Pogue, David, *The Twitter Experiment*, N.Y. Times (Jan. 29, 2009) <nytimes.com/2009/01/29/technology/personaltech/29pogue-email.html?pagewanted=print>; Baldas, Tresa, *Beware: Your 'tweet' on Twitter could be trouble*, Nat'l L.J. (Dec. 22, 2008) <law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202426916023>. *See also* Mark Magnier, *Tweet lands Indian official in hot water*, L.A. Times (Jan. 2, 2010) <sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/03/BUCE1BC091.DTL&type=printable>.

[41] In *Marshall v. Mayor of Savannah*, 2010 U.S. App. LEXIS 3233 (11th Cir. Feb. 17, 2010) <ca11.uscourts.gov/unpub/ops/200913444.pdf>, a federal circuit court wrestled with the viability of a disparate treatment claim in the context of Web 2.0 postings by a female employee and some of her co-workers. On her MySpace page, a female firefighter posted inappropriate photographs, including two of fellow firefighters and two revealing ones of her. Shel had not sought permission to use or post the photographs of the others. The revealing photographs of her were purportedly taken for modeling purposes. During a departmental meeting to discuss her photos, Plaintiff was defensive and combative, and her superiors decided her "insubordination" warranted termination. Thereafter, she sued, alleging gender, race and national origin Title VII discrimination. Plaintiff maintained that male firefighters in the Department had posted unauthorized photos of Savannah firefighters, yet she was being singled out for discipline for her postings. Yet, when she asked to identify the male firefighters, she refused. The court held that, because the Department did not have any knowledge of other firefighters (whether male or female) participating in the same activity, Plaintiff could not prove her *prima facie* case; and it thus granted summary judgment in favor of the Department. *Id.* at *17-18.

[42] *See* Rob Pegoraro, *Bing brings Facebook-fueled search results*, Wash. Post (Oct. 13, 2010) <voices.washingtonpost.com/fasterforward/2010/10/bing_brings_facebook-fueled_se.html>; Thomas Claburn, *Google Launches Social Search*, Info. Week (Oct. 27, 2009) ("searchers are more likely to find what friends and associates have to say") <informationweek.com/shared/printableArticle.jhtml;jsessionid=X2SFWWL1CJBP3QE1GHOSKH4ATMY32JVN?articleID=220900747>; Alexei Oreskovic, *Twitter in Google, Microsoft licensing talks: report,* Reuters (10/8/09) <reuters.com/articlePrint?articleId=USTRE5974C420091008>; *New Real Time Search Engine [Scoopler.com] Aggregates Web 2.0 Content*, beSpacific (5/10/09) <bespacific.com/mt/archives/021321.html#021321>.

[43] *See* Matt Raymond, *How Tweet It Is!: Library [of Congress] Acquires Entire Twitter Archive*, Library of Congress Blog (April 14,2010) <blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/>; Jeffrey Rosen, *The Web Means the End of Forgetting*, The New York Times (July 19, 2010) <www.nytimes.com/2010/07/25/magazine/25privacy-t2.html>.

[44] *See* the agreements and technologies discussed in the resources cited in note 42 supra.

changes in, social-media sites' privacy settings.[45] Some social media content about employees is even outside the employees' own control, making it even more difficult for employers to regulate.[46] Employers' risks of damaging disclosures have thus greatly increased.

Many of the pros and cons of employer-sponsored social-media sites[47] are in the resources cited/linked at Slides 12-20 of Appendix F (including two public-sector lists at the bottom of Slide 15[48]). In addition, those interested in the growing body of social-media ethical prohibitions as to lawyers, jurors and judges should use Appendix E.

---

[45] For specific examples of policy changes, *see* ACLU Guide to New Facebook Privacy Controls (Aug. 25, 2011) <www.aclu.org/blog/technology-and-liberty/aclu-guide-new-facebook-privacy-controls>; Facebook, *Making It Easier to Share With Who You Want* (Aug. 23, 20110) <https://blog.facebook.com/blog.php?post=10150251867797131>; Somini Sengupta, *New Control Over Privacy on Facebook*, N.Y. Times (Aug. 23, 2011) <www.nytimes.com/2011/08/24/technology/facebook-aims-to-simplify-its-privacy-settings.html>; Kelly Fiveash, *Google: Go Public on Profiles or We'll Delete You*, The Register (July 7, 2011) <www.theregister.co.uk/2011/07/07/google_profiles_no_longer_private/> (describing a Google privacy policy change); Josh Constine, *Facebook Alerting Users to Facial Recognition Privacy Setting with Home Page Ads*, Inside Facebook (June 15, 2011) <www.insidefacebook.com/2011/06/15/facial-recognition-home-page-ads-tag-suggest/> (discussing a new default privacy setting on Facebook). For general information about privacy settings, *see* Symantec Corp., *Protecting Your Privacy on Social Media Networks*, Club Norton <http://us.norton.com/clubsymantec/library/article.jsp?aid=cs_protecting_your_privacy> (last visited Oct. 22, 2011); Kathy Kristof, *6 Things You Should Never Reveal on Facebook*, Yahoo!® Finance (Sep. 14, 2010) <http://finance.yahoo.com/family-home/article/110663/6-things-you-should-never-reveal-on-facebook>; *ReclaimPrivacy Launches Facebook Privacy Settings Tool – Privacy – Info. Week*, Future Lawyer (May 18, 2010) <http://Fut-Law-5-10.notlong.com> (linking to <http://InfoWeek-5-10.notlong.com>, which links to the Reclaim tool itself at <http://www.reclaimprivacy.org>); *7 Things to Stop Doing Now on Facebook*, Consumer Reports (May 12, 2010) <http://finance.yahoo.com/family-home/article/109538/7-things-to-stop-doing-now-on-facebook>; Alison Driscoll, *FACEBOOK FAIL: How to Use Facebook Privacy Settings and Avoid Disaster*, Mashable (Apr. 28, 2009) <http://mashable.com/2009/04/28/facebook-privacy-settings/>.

[46] Prime examples are tagged content, such as photos on Facebook and videos on Google's YouTube. *See* Kevin J. O'Brien, *Germany Investigating Facebook Tagging Feature*, N.Y. Times (Aug. 3, 2011) <http://www.nytimes.com/2011/08/04/technology/germany-investigates-facebook-tagging.html>; *EU PROBES FACEBOOK'S FACIAL RECOGNITION*, Bytes in Brief (July 2011) <http://www.senseient.com/publications/bytes/html/July_2011.html>; John Diaz, *An in-your-face technology*, S.F. Chronicle (June 12, 2011) <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/06/12/INRB1JQN05.DTL>; Stephanie Bodoni, *Facebook to Be Probed in EU for Facial Recognition in Photos*, Bloomberg BusinessWeek (June 8, 2011) <http://www.businessweek.com/news/2011-06-08/facebook-to-be-probed-in-eu-for-facial-recognition-in-photos.html>. Emil Protalinski, *Court: tagging Facebook photos without permission is okay*, ZDNet (Mar. 18, 2011) <http://www.zdnet.com/blog/facebook/court-tagging-facebook-photos-without-permission-is-okay/819>; *Lalonde v. Lalonde*, No. 2009-CA-002279-MR (Ky. Ct. App. Feb. 25. 2011) <http://162.114.92.72/COA/2009-CA-002279.pdf>; ARMA, *EU Investigates Facebook, Google Tagging*, Info. Mgmt. (July-Aug 2010) ("personal data transfers" may violate European laws) <http://content.arma.org/IMM/JulyAug10/IMM0710upfront.aspx>.

[47] For an introduction to these issues both on the external web and on intranet sites, *see* Heather A. Hoyt, *Monitoring the Virtual Water Cooler: Employees on Facebook and More*, Business Management Daily (July 10, 2011) <http://www.businessmanagementdaily.com/articles/26209/1/Monitoring-the-virtual-water-cooler-Employees-on-Facebook-and-more/Page1.html> (describing IBM's encouragement of social media use); Verne G. Kopytoff, *Companies are Erecting In-House Social Networks*, N.Y. Times (June 26, 2011) <http://www.nytimes.com/2011/06/27/technology/27social.html>; Ashlee Vance, *Yammer, Chatter, Hot Water: Corporate Social Networks Have Advantages—and Perils*, BusinessWeek (April 28, 2011) <http://www.businessweek.com/magazine/content/11_19/b4227031833107.htm> (quoting Robert Brownstone).

[48] As to governmental agencies, *see also* ACT-IAC Collaboration & Transformation (C&T) Shared Interest Group (SIG), *Best Practices Study of Social Media Records Policies* (Mar. 2011) <http://ACT-IAC-SIG-Mar-11.notlong.com>; Alice Lipowicz and William Jackson, *Facebook gets friendlier for state, local organizations; NASCIO, state attorneys general negotiate new terms of service for agencies*, Gov't Computer News (Jan. 6, 2011) <gcn.com/articles/2011/01/06/facebook-removes-barriers-to-state-and-local-agency-participation.aspx>; Wash. State A.G., *Attorneys General, NASCIO announce deal to improve terms for state, local entities using Facebook*, News Release (Jan. 5, 2011) <atg.wa.gov/pressrelease.aspx?id=27120>; National Association of State Chief Information Officers (NASCIO), *A National Survey of Social Media Use in State Gov't* (Sep. 28, 2010) <nascio.org/publications/documents/NASCIO-SocialMedia.pdf>; Jana Hrdinová, Natalie Helbig and Catherine Stollar Peters, *Designing Social Media Policy for Government: Eight Essential Elements*, CTG (May 2010) <ctg.albany.edu/publications/guides/social_media_policy/social_media_policy.pdf>; Web Content Managers Forum (WCMF), *Terms of Service Agreements* (Jan. 14, 2010) <forum.webcontent.gov/?page=TOS_agreements>. *See also* WCMF, *[Federal] Agency Points of Contact for Terms of Service Agreements* <forum.webcontent.gov/?page=TOS_TYagencyPOCs>.

i. Day-to-day Issues *(c't'd)*

TIP: One approach when modernizing a TAUP to address social-networking sites is to cover this set of topics:

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

A. General Guidelines

B. Specific Guidelines

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

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

---

ii. eDiscovery of Social-Media Postings

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.[49] E-discovery pertaining to emails and electronic documents has been commonplace in litigation for some time.[50] However, posts, tweets, texts and "private" Facebook and MySpace messages are now additional targets of production requests and subpoenas.[51]

---

[49] Anna Scott, *Mining Social Media Sites for Litigation Gold Courts Still Sorting Out Rules As Parties Increasingly Dig Up Dirt From Online Networks*, D.J. (Oct. 1, 2010), purchasable via subscription at <http://www.dailyjournal.com/subscriber/index.cfm?cat=search>.

[50] *See generally* various articles linked off of <fenwick.com/attorneys/4.2.1.asp?aid=544#publications>.

[51] The ensuing textual discussion regarding *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007) <ecf.nvd.uscourts.gov/doc1/11511167020> is adapted from Victor Schachter, Michael Sands, Robert D. Brownstone & Sheeva Ghassemi-Vanni, *POSTS, TWEETS, TEXTS AND POKES*, at 21-22 (Sep. 2010).

In the past year or so, judges have become even more aggressive in granting wide-ranging judicial and adversarial access to a litigant's "private" social media posts and messages.[52] For example, in *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*,[53] the court analyzed whether Plaintiff could be compelled to produce private MySpace email messages. Plaintiff sued Defendants for sexual harassment, among other causes of action, under Title VII and Nevada state law. During the course of the *Mackelprang* litigation, Defendants discovered that Plaintiff maintained two separate MySpace accounts. Believing the private email messages contained in her MySpace accounts might have identified issues relating to her lawsuit, Defendants sought to compel production of all private email communications from her MySpace accounts. Both Plaintiff and MySpace refused to comply with the requests.

The court recognized that ordering Plaintiff to produce all of the private email messages in her MySpace accounts "would allow Defendants to cast too wide a net for any information that might be relevant and discoverable."[54] Thus, although Defendants were not entitled to all email messages in Plaintiff's MySpace accounts, they were entitled to relevant email communications – excluding any messages "between Plaintiff and third persons regarding allegedly sexually explicit or promiscuous emails not related to Plaintiff's employment."[55]

---

[52] Some of the key decisions in this area are compiled in Appendix B. In the employment litigation context, *see, e.g., Coface Collections North America, Inc. v. Newton*, 2011 WL 2176196 (3d Cir. June 6, 2011) (affirming preliminary injunction to plaintiff in non-compete clause dispute when Defendant, a former officer and consultant of Plaintiff, had recruited employees using Facebook) <http://vls.law.villanova.edu/locator/3d/June2011/111482np.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>. In other contexts, *see Largent v. Reed*, No. 2009-1823 (Pa. Ct. Common Pleas Franklin Cty. 11/8/11) (granting disclosure of party's public Facebook information in personal injury case) <http://druganddevicelaw.net/Opinions%20in%20blog/Largent.pdf>; *Matter of Progressive Ins. Co. v. Herschberg*, 2011 NY Slip Op 31288(U), (N.Y. Sup. Ct. Mar. 30, 2011) (granting temporary stay of arbitration when respondent's testimony that he suffered from physical disabilities contradicted portions of his Facebook page, including photos in an album titled "Another day of play… I gotta get a job!") <http://www.courts.state.ny.us/Reporter/pdfs/2011/2011_31288.pdf>; *McCann v. Harleysville Ins. Co, of N.Y.*, 78 A.D.3d 1524, 910 N.Y.S.2d 614 (4 A.D. Nov. 12, 2010) (disallowing "fishing expedition" absent factual predicate for relevancy; but finding abuse of discretion in protective order that blocked all future Facebook requests) <nycourts.gov/reporter/3dseries/2010/2010_08181.htm>; *Romano v. Steelcase*, 907 N.Y.S. 2d 650, at *5 (N.Y. Sup. Sept. 21, 2010) ("[t]o deny Defendant an opportunity access to these sites not only would go against the liberal discovery policies of New York favoring pre-trial disclosure, but would condone Plaintiff's attempt to hide relevant information behind self-regulated privacy settings") <courts.state.ny.us/Reporter/3dseries/2010/2010_20388.htm>; *Barnes v. CUS Nashville, LLC, [d/b/a Coyote Ugly Saloon]*, 2010 WL 2265668 (M.D. Tenn. June 3, 2010) (in slip and fall case, offering to create temporary Facebook account to "friend" Plaintiff's friends/witnesses "for the sole purpose of reviewing photographs and related comments in camera") <https://ecf.tnmd.uscourts.gov/doc1/16911303989>. *See also U.S. v. Phaknikone*, 605 F.3d 1099. 1107 (11th Cir. 2010) ("*The Evidence About Phaknikone's MySpace Account Was Inadmissible Character Evidence, but Its Admission Was Harmless.")* <ca11.uscourts.gov/opinions/ops/200910084.pdf>. *See generally* Nadine R. Weiskopf, *Tweets and Status Updates Meet the Courtroom: How Social Media Continues to be a Challenge for E-Discovery in 2011*, LEXIS (Sep. 12, 2011)<lexisnexis.com/eMarketing_WCS_graphics/145833/Social-Media-and-eDiscovery-Weiskopf.pdf>; Terry Baynes, *Would You 'Friend' the Judge?* The American Lawyer (Oct. 26, 2010*)* <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202473899448>*;* Nadine R. Weiskopf, *Social Media and E-Discovery: New Tools and New Challenges*, LEXIS (Sep. 16, 2010) <lexisnexis.com/eMarketing_WCS_graphics/139920/socialMediaAndE-Discovery.pdf>. *See also* the additional Internet eDiscovery decisions discussed in Michelle Sherman, *Social Media Poked in Discovery*, Recorder (Dec. 23, 2010) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202476547045>.

[53] *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>.

[54] *Id.* at *21.

[55] *Id*. at *25-26.

More recently, in May of 2010, a judge in the U.S. District Court for the Central District of California overruled a magistrate judge's production order by holding that private communications through social networking websites and web hosting services are protected under the federal Stored Communications Act (SCA).[56] The case, *Crispin v. Christian Audigier, Inc.*, No. CV 09-09509 MMM (JEMx) (C.D. Cal. May 26, 2010) <https://ecf.cacd.uscourts.gov/doc1/031110245153>, involved a copyright dispute whereby Crispin, an artist, alleged that Audigier, a clothing designer, exceeded the rights granted by an oral agreement for use of his graphics on Audigier's products.

During litigation, Audigier and other defendants subpoenaed Facebook, MySpace and Media Temple, Inc. (a web hosting service) for communications to or from Crispin relating to Audigier, to determine the nature of the agreement. Crispin, arguing that the subpoenas sought SCA-protected communications, filed an *ex parte* motion to quash the subpoenas. The magistrate judge denied the motion. The District Court reversed, holding that each of Facebook, MySpace and Media Temple, Inc. was an "electronic communication "service" as defined by the SCA, thus preventing the requested disclosures. Although the court held that the private communications were protected by the SCA, it has yet to resolve whether Crispin intended communications on his wall or comment sections to be private.[57]

A series of 2010 and 2011 Pennsylvania state a case has highlighted the current uncertainty about whether a court will allow discovery of "private" social media content.[58] Pennsylvania courts have allowed discovery of "private" posts once publicly available content is inconsistent with that party's statements to the court.[59] In *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD (C.P. Jefferson Sep. 9, 2010) <ediscoverylaw.com/uploads/file/McMillen%20v%20Hummingbird%20Speedway.pdf> the court ordered a personal injury Plaintiff to "provide his Facebook and MySpace user names and passwords to counsel for Defendants" because "[w]here there is an indication that a person's social network sites contain information relevant to . . . a lawsuit, . . . and given . . . the law's general dispreference [sic] for the allowance of privileges, access to those sites should be freely granted"). In *Zimmerman v. Weis Markets, Inc.*, PICS Case No. 11-0932 (C.P. Northumberland May 19, 2011) <gtleblog.com/uploads/file/Zimmerman.pdf>, another Pennsylvania personal injury case, the defendant was permitted to discover non-public portions of Plaintiff's Facebook and MySpace pages. The plaintiff had alleged that scars from a workplace injury left him too embarrassed to wear shorts, but public portions of his Facebook page included pictures of Plaintiff wearing shorts. The judge granted the motion to compel, adopting the reasoning of *McMillen* and finding that Pennsylvania does not recognize a privilege for information posted on private sections of websites. *Id.*

---

[56] As to the SCA generally, *see* Section II(B)(1)(a) below.

[57] A recent Florida case relied on *Crispin* in holding that an employee had standing to quash third-party subpoenas on Facebook and MySpace, but also held that because Facebook and MySpace are not located in Florida, the court lacked the authority to quash the subpoenas issued to those sites. *Mancuso v. Florida Metropolitan Univ.*, 2011 WL 310726 (S.D. Fla. Jan. 28, 2011) <http://docs.justia.com/cases/federal/district-courts/florida/flsdce/0:2009cv61984/349087/142/0.pdf>. There, an employee had filed an FLSA suit, seeking back overtime wages from his university-system employer. The employer then sought a subpoena for the employee's records from Facebook and MySpace.

[58] *See* Vianei Lopez Robinson, *Digging Up Social Media's Treasure Trove of Discovery*, Texas Lawyer (July 11, 2011) <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202499810802> (discussing *Zimmerman*); Jeremy Byellin, *An Order to Disclose Your Facebook Password?* Westlaw Insider (June 2, 2011) <westlawinsider.com/social-media-law/an-order-to-disclose-your-facebook-password/>; Gina Passarella, *The Evolution of Social Media Discovery in Pennsylvania,* The Legal Intelligencer (May 27, 2011) <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202495346037> (discussing *McMillen*, *Zimmerman*, and *Piccolo*).

[59] *See also Purvis v. Commissioner of Social Security*, 2011 WL 741234 (D. N.J. Feb. 23, 2011) <http://scholar.google.com/scholar_case?case=3695101701318980368> (when plaintiff applied for supplemental Social Security income claiming disability due to asthma, noting that "[a]lthough the Court remands the ALJ's decision for a more detailed finding, it notes that in the course of its own research, it discovered one profile on what is believed to be Plaintiff's Facebook page where she appears to be smoking. … If accurately depicted, Plaintiff's credibility is justifiably suspect.").

But another Pennsylvania court barred "private" Facebook information from discovery. In *Piccolo v. Paterson*, No. 2009-04979 (Pa. Ct of Common Pleas; May 5, 2011) <theemployerhandbook.com/piccolo.PDF>, the judge entered a one-paragraph order denying the plaintiff's motion to compel discovery of "private" Facebook content. In response to the defendant's motion seeking discovery, the plaintiff had noted that – unlike the plaintiffs in *McMillen* and *Zimmerman* – Piccolo's intra-lawsuit assertions were not inconsistent with statements she had on the publicly viewable portion of her Facebook page.[60]

All of the above-described rulings indicate that, while some aspects of social networking websites remain cloaked in privacy, these modern venues are now part of the discovery milieu.

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.[61]

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.[62] This 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.

II. MONITORING OF EMPLOYEES' ELECTRONIC ACTIVITIES

A. Introduction

The most publicized workplace monitoring issue this decade has been comprised of the surveillance, retrieval and review of employee use of e-mail systems and Internet connections.[63] Courts have generally upheld employer interests in monitoring the use of their computer systems. While the case law recognizes an employer's right to monitor employee use of the company network, traditional labor and employment law may restrict the employer's ability to act upon that information in formulating employment decisions.

---

[60] Gina Passarella, *Facebook Postings Barred from Discovery*, The Legal Intelligencer (May 17, 2011) <http://www.law.com/jsp/pa/PubArticlePA.jsp?id=1202493920630>.

[61] 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/>.

[62] 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* 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/>.

[63] *See* Brownstone eWorkplace, supra note 2, at 16-17 (.pdf pp. 22-23) <http://White-Paper-8-09-at-22.notlong.com>.

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 developments from the past two years as to those five respective issues are discussed below *seriatim*. For a fuller treatment of the pre-2009 legal standards in these areas, *see* Brownstone eWorkplace, supra note 2, at 17-44 (.pdf pp. 23-50) <http://White-Paper-8-09.notlong.com>.

1. Federal Electronic Communications Privacy Act 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 employer's right to retrieve and read such e-mails.[64] Note, however, that potential SCA violations *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.[65]

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.[66] Many of these employees may not realize that such activity leaves electronic footprints on the hard drives of company-

---

[64] *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) (affirming grant of summary judgment against Plaintiff, an independent insurance agent alleging that Defendant insurance company had retrieved from digital storage an e-mail Plaintiff had sent, and which had been received by its intended recipient); *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183 (S.D. Cal. 2008) (granting summary judgment for Defendant/employer on SCA and invasion of privacy claims). *Cf. Theofel v. Farey-Jones,* 359 F.3d 1066, 1075-76 (9th Cir. 2004) (in case outside the employment context, reinstating a dismissed SCA claim and disagreeing with some of *Fraser*'s statutory interpretation). *See generally* Brownstone, Robert D., 9 *Data Security & Privacy Law, Privacy Litig.* Ch. § 9:29 (West 2008 & Supp. 2010).

[65] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879–80 (9th Cir. 2002) (where airline executive accessed employee/pilot's password-protected personal site via passwords executive had obtained from other pilots, reversing summary judgment in favor of employer and finding material issues of fact regarding authorized-user exception of 18 U.S.C.A. § 2702(c)(2)); *Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 925–26 (W.D. Wis. 2002). As a practical matter, as discussed in detail in Section II(B)(1)(a)(i) above, 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.*

[66] 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.

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.[67]

Moreover, the server receiving an offending e-mail (perhaps a sexually harassing message sent from an employee of one company to an employee of another company) can trace back the source. Then, one could identify, at the least, the server that dispatched the e-mail and perhaps also trace its origin to the precise machine generating the message (depending on how the network software and hardware are configured). Because employees would presumably access these services using their employers' computers and Internet connections, it is likely a court will find that these communications are no more protected under anti-wiretap laws than e-mail sent over a company's servers. 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.[68]

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

However, 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.[69] 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.[70] In 2008, the Southern District of New York prohibited an employer from using in litigation e-mails that a former employee had sent to his attorney and others via a private, web-based account from his work computer. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) <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>). In that the employer's e-mail policy did not expressly provide notice of monitoring employees' web-based

---

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

[68] *See generally* <digitaldueprocess.org/>. *See also* Tamar Gubins, *Electronic Privacy Law Needs a Facelift*, Daily J. (Apr. 9, 2010) <aclunc.org/news/opinions/electronic_privacy_law_needs_a_facelift.shtml>.

[69] *See, e.g.*, the many decisions gathered in Appendix C. *Cf. Transocean Capital, Inc. v. Fortin*, 21 Mass. L. Rptr. 597, 2006 WL 3246401 (Mass. Super. Ct. Oct. 20, 2006) (though finding waiver for other reasons, court found employer had not shown that it had actually adopted HR policies administered by third-party provider – such that mere "us[e] the Company's email address and computer system" insufficient to waive privilege).

[70] *See generally* Michael F. Urbanski and Timothy E. Kirtner, *Employee Use of Company Computers – A Privilege Waiver Mine Field* , 57 Va. Lawyer 40 (Feb. 1, 2009) <http://www.vsb.org/docs/valawyermagazine/vl0209_computers.pdf>; Herrington, Matthew J. and Gordon, William T.*, 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 (May 5, 2008) <http://7PVSLR18-685.notlong.com>. *But see Long v. Marubeni America Corp.*, 2006 WL 2998671, at *1, *3 (S.D.N.Y. Oct. 19, 2006) (where temporary internet files contained "residual images of . . . e-mail messages" sent by employees to their attorney 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 is clear and unambiguous[; P]laintiffs disregarded the admonishment voluntarily and, as a consequence, have stripped from the e-mail messages . . . the confidential cloak") <wolfs2cents.files.wordpress.com/2007/03/usdc-sdny_long_v_marubeni2006usdistlex76594_19oct.pdf> ; *Scott v. Beth Israel Med. Ctr.*, 17 N.Y. Misc. 3d 934, 2007 N.Y. Slip Op. 27429 (N.Y. Sup. N.Y. Oct. 17, 2007) (distinguishing *Jiang*, in employment breach of 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" e-mail policy combined with stated policy allowing for employer monitoring).

accounts, the court found the employee had a reasonable expectation of privacy in the e-mails. That opinion is exemplary of many decisions reflecting the importance of a usage policy evincing clear, broad coverage.

In recent years, some of the decisions on this attorney-client issue have been very solicitous toward the respective employee.[71] In March 2010, the New Jersey Supreme Court, in *Stengart v. Loving Care Agency, Inc.,* agreed with an intermediate appellate court that had accepted the employee's privilege argument.[72] The New Jersey high court found that the employee had a reasonable expectation of privacy in e-mails sent to and from her attorney on her company laptop – such that the attorney-client privilege continued to protect such communications. The employee had used her company-issued laptop to exchange e-mails with her attorney through her personal Yahoo e-mail account; and she later filed a discrimination lawsuit against her former employer. The former employer subsequently retrieved the e-mails through a forensic expert.

Under the *Stengart* reasoning, the communications remained protected from review by the employer due to the strong attorney-client privilege public policies. The court also noted that, even if the company policy had explicitly informed the employee not only that she could not use the laptop for personal purposes but also attorney-client communications were subject to employer retrieval and review, the policy would *still* not have been enforceable as to communications sent through *personal, password-protected* e-mail accounts.

In late 2009, applying New York law, the District Court for the District of Columbia upheld the claim of privilege by a federal Department of Justice employee, because it found:

---

[71] *See, e.g., United States v. Hatfield*, 2009 U.S. Dist. LEXIS 106269, *26-27 (E.D.N.Y. Nov. 13, 2009) (despite employer Computer Usage Policy's express warnings that employees should use their computers solely for "business purposes" and that they "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>. *Compare 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") <https://ecf.ilnd.uscourts.gov/doc1/06718389059> or <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2009cv06974/237454/122/0.pdf>.

[72] *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. Mar. 30, 2010) <http://www.judiciary.state.nj.us/opinions/supreme/A1609StengartvLovingCareAgency.pdf>, *affirming and modifying* 408 N. J. Super. 54, 973 A.2d 390, 393 (N.J. App. Div. June 26, 2009) ("the policies undergirding the attorney-client privilege substantially outweigh the employer's interest in enforcement of its unilaterally imposed regulation") <http://lawlibrary.rutgers.edu/decisions/appellate/a3506-08.opn.html>, *reversing* 2009 WL 798044 (N.J. Super. L. Div. Feb. 5, 2009), available at <http://privacyblog.littler.com/uploads/file/Stengart%20v%20Loving%20Care.pdf>. For commentaries on the highest court decision, *see* F&W Emp Brief (Apr. 13, 2010) <http://www.fenwick.com/publications/6.5.4.asp?mid=57&WT.mc_id=EB_041310#nb>, on which the above discussion is partially based and *see also* the articles cited/linked at page C-3 of Appendix C. The now-reversed lower court decision was discussed in 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 (Mar. 24, 2009) <http://privacyblog.littler.com/2009/03/articles/electronic-resources-policy/webbased-email-accounts-accessed-at-work-private-or-not-look-to-the-handbook/print.html>; Fernando M. Pinguelo and Andrew K. Taylor, *New Jersey Court Finds Waiver of Privilege in 'Loving' Way*, (Apr. 14, 2009) <http://www.discoveryresources.org/case-law-and-rules/new-jersey-court-finds-waiver-of-privilege-in-%e2%80%98loving%e2%80%99-way/print/>; Mary Pat Gallagher, *E-Mail Sent on Company Laptop Waives Privilege*, N.J.L.J. (Mar. 10, 2009) <law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428912956&rss=ltn>

> [his] expectation of privacy was reasonable. The DOJ … policy … does not ban personal use of the company e-mail. Although the DOJ does have access to personal e-mails sent through this account, [he] was unaware that they would be regularly accessing and saving e-mails sent from his account.[73]

And, in 2009, in lengthy dicta, a Maine high court decision took in-house counsel to task for reviewing a privileged memorandum found on its former president's work laptop.[74] Yet, in that same Maine case, a concurring opinion took a diametrically opposed view, finding that, because he was "fully cognizant of" a no-expectation-of-privacy, the former employee had "accepted the risk" that an e-mail attachment forwarded to his "business e-mail and placed on his business computer, might become known to" his employer.[75]

On the other hand, the outcomes continue to diverge, with several decisions over the past two years rejecting in whole or in part an (ex-) employee's arguments that attorney-client privilege trumped a no-expectation-of-privacy policy.[76] Most recently, in a California Court of Appeals decision, *Holmes v. Petrovich*,[77] the court found that emails sent by an employee to her attorney on a work computer were not attorney-client privileged because they were sent from a work email account.[78] That opinion is now part of a group of at least 16 nationwide decisions since 2005 addressing whether an employer's No-Employee-Expectation-of-Privacy-Policy (NoEEPP)/Technology-Acceptable-Use-Policy (TAUP) trumps an individual employee's attorney-client privilege rights.[79]

In *Holmes*, Plaintiff was hired as an executive assistant to the head of a company. Shortly thereafter, she informed her boss that she was pregnant. Her boss became upset at this disclosure, and exchanged a series of emails with Plaintiff indicating that, while he did not intend to violate any laws, he felt taken advantage of. In response, Plaintiff used her work email account to send emails to an outside

---

[73] *Convertino v. U.S. DOJ*, 674 F. Supp. 2d 97 (D.D.C. 2009) <https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2004cv0236-167>.

[74] *Fiber Materials, Inc. v. Subilia*, 974 A.2d 918, 928 (Me. 2009) <http://www.courts.state.me.us/court_info/opinions/2009%20documents/09me71fi.pdf>.

[75] *Id.* at 929 (concurring in part) (privilege waived because "disclosure may have been ill considered but was not inadvertent"). *See also* BNA Privacy & Security Law Report, *Corporate Counsel Are Criticized for Using Sensitive Memo Found on Company Laptop*, 8 PVLR 1093 (BNA July 27, 2009), available by subscription at <http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=14097996&vname=pvlrnotallissues&fn=14097996&jd=a0b9b8y5e4&split=0>. In the public employer context, though, even if common law and/or SCA claims do not succeed there still may be a Fourth Amendment claim.

[76] *Alamar Ranch, LLC v. County of Boise*, 2009 U.S. Dist. LEXIS 101866, 2009 WL 3669741 (D. Idaho Nov. 2, 2009) (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. Sep. 23, 2009) (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") <https://ecf.flsd.uscourts.gov/doc1/05117071717>.

[77] *Holmes v. Petrovich*, 191 Cal. App. 4th 1047, 119 Cal. Rptr. 3d 878 (3 Dist. 1/13/11) <http://www.courtinfo.ca.gov/opinions/archive/C059133.PDF>.

[78] This decision and other cutting-edge decisions are discussed in Robert D. Brownstone, Sheeva J. Ghassemi-Vanni & Soo Cho, *Privacy of Email and Text Messages – Case Law Sprinting to Catch Up to Modern Technology*, Privacy & Info. L. Rep., Bloomberg (Mar. 2011) <fenwick.com/docstore/Publications/EIM/fenwick_west_brownstone_ghassemi-vanni_cho_article.pdf>.

[79] *See* Appendix C § I, at C-1 to C-2

attorney, indicating, among other things, her view that she was working in a hostile environment. Plaintiff eventually emailed her boss to inform him that his feelings regarding her pregnancy left her with no alternative but to end her employment.

Thereafter, Plaintiff filed a suit for sexual harassment, retaliation, wrongful termination, violation of right to privacy, and intentional infliction of emotional distress. At trial, the jury was shown several emails between Plaintiff and her attorney. Plaintiff had argued that these emails were attorney-client privileged. However, the trial court had ruled that Plaintiff's emails, sent on a company computer and via the employer's email system, were not protected by the attorney-client privilege because they were not private. The court found support in the language of the company's detailed computer usage policy, which stated in unambiguous terms that:

- Company technology resources should be used only for company business and employees are prohibited from sending or receiving personal emails;
- Employees have no right to privacy for personal information created on company computers;
- Email is not private communication;
- The Company may inspect all files or messages at any time; and
- The Company would periodically monitor technology resources for compliance with Company policy.[80]

On appeal, the court affirmed the decision of the trial court, concluding that the pertinent email messages did not constitute "confidential communications between client and lawyer" because Plaintiff knew of the company policy regarding no personal use, she had been warned that the company would monitor its computers for compliance with company policy, and she was warned that she had no right of privacy as to messages created on company computers. The court described the communications as "akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him."[81]

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.

---

[80] *Holmes*, 119 Cal. Rptr. 3d at 896-97.

[81] *Id*. at 896.

c. ECPA Limits on Intrusions into Workers' Private Accounts

If there is no actual trail left on an employer's system or computer, then an employer should not go as far as to actually log into and/or access an (ex-)employee's personal webmail account. In 2009, one federal circuit found that, as a result of such unlawful access, actual damages and/or punitive damages may be recoverable.[82] Also in 2009, a federal district court found that a viable federal Wiretap Act claim was stated where Plaintiff alleged that his employer used a "keylogger" to record his "keystrokes entering his email password" – and then used that password to "log[ ] into his personal email account, and read his personal email."[83] Previously, in 2007, a District Court judge in Texas had held that individuals even have a legally cognizable privacy interest in the numbers they dial on their cell phones, in the context of an employer-hired investigator who had obtained from a provider numbers dialed by some former employees.[84]

In 2009, yet another federal decision upheld a jury verdict against an employer that had overreached when it logged into and reviewed an access-restricted Web 2.0 page containing posts by multiple employees.[85] In *Pietrylo v. Hillstone Restaurant Group*, a server at a restaurant in New Jersey created a MySpace.com group whose purpose was to let current and former employees "vent" about their experience while working at the restaurant. The user group was invitation-only and required a password to enter and view the postings. The page included posts containing vulgar and sexually explicit comments as well as references to violence and illegal drug use. Eventually, a manager of the restaurant learned of that group page and asked a hostess (who had been invited to join the group) to provide him with her personal login information so he could access the page. Although the manager made no threats against her if she refused, the hostess testified that she thought she "would have gotten in some sort of trouble" if she had refused to cooperate. Shortly thereafter, the company terminated plaintiffs based on their comments on the site and involvement in creating it.

Plaintiffs sued in federal district court in New Jersey, alleging, among other claims, terminations in violation of public policy, invasion of privacy and violations of the federal Stored Communications Act (SCA) and parallel state statutes. A jury found that the restaurant's managers had violated federal and state laws that protect the privacy of online communications, and awarded plaintiffs $3,400 in back-pay and $13,600 in punitive damages. Specifically, the jury determined that the company violated the SCA and parallel state provisions in the way that it had gained access to the MySpace postings, namely management requesting and using the hostess' password to access the site. The jury, however, rejected plaintiffs' privacy claims,

---

[82] *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>. *See also* footnote 65 supra (discussing *Konop* and *Fischer*). *See also* Marcia Coyle, *Landmark Ruling in E-Mail Theft Case*, Nat'l L. J. (Mar. 26, 2009), available by subscription at <http://www.law.com/jsp/ca/PubArticleFriendlyCA.jsp?id=1202429394819>.

[83] *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>.

[84] See *McEwen v. SourceResources.com*, 2007 U.S. Dist. LEXIS 10156 (S.D. Tex. Feb. 13, 2007) (under the SCA and the Wiretap Act, the numbers dialed on a cell phone constitute "transfer of … data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.") <https://ecf.txsd.uscourts.gov/cgi-bin/show_doc.pl?caseid=464830&de_seq_num=140&dm_id=4692266&doc_num=43&pdf_header=1>.

[85] *See generally Jury Finds Employer Accessed "Private" MySpace.com Group Page In Violation Of The Federal Stored Communications Act*, F&W Emp. Brief (Sep. 9, 2009) <fenwick.com/docstore/publications/Employment/EB_09-09-09.pdf#page=3>, from which part of the ensuing discussion is adapted. *Compare* Gordon, supra note 62 as to accusation that Maryland state agency had violated SCA by asking job applicants to disclose Facebook password (citing ACLU, *Letter to Md. Dep't of Pub. Safety & Correctional Servs.* (Jan. 25, 2011) <privacyblog.littler.com/uploads/file/ACLU%20Letter%20Jan%2025%202011%20Maryland%20Dept%20of%20Corrections.pdf>.

explaining that plaintiffs did not have a reasonable expectation of privacy in the MySpace group page. The jury also rejected plaintiffs' claims for damages suffered as a result of emotional distress.

Shortly thereafter, the trial judge rejected the employer's challenges to the verdict. *See Pietrylo v. Hillstone Rest. Group d/b/a Houston's*, 2009 WL 3128420, at *6, 29 IER Cases 1438 (D.N.J. Sep. 25, 2009) (Opinion denying "Defendant's motion for judgment as a matter of law pursuant to Fed.R.Civ.P. 50(b) or, in the alternative, for a new trial pursuant to Fed.R.Civ.P. 59"). <https://ecf.njd.uscourts.gov/doc1/11914223001>. A month later, the employer filed a notice of appeal. *See* <https://ecf.njd.uscourts.gov/doc1/11914299632>. However, a few months thereafter (in early 2010), the appeal was dismissed upon stipulation of the parties. *See* <https://ecf.njd.uscourts.gov/doc1/11914518287>.

In contrast to *Van Alstyne*, *Pietrylo* and the other decisions cited in this sub-section, *see* Section V(B)(1)(a) below for a discussion of a state court appellate decision – *Sitton v. Print Direction, Inc.*, __ S.E. 2d __2011 WL 4669712 (Ga. App. Sep. 28, 2011) <http://tinyurl.com/Sitton-Print-Ga-App-9-28-11> -- that 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 SCA Circuit opinions, one employment-related and one not.[86] Each of those cases – *Quon* and *Warshak* – was then ultimately litigated to a final judgment; and each resulted in a ground-breaking decision – *on Fourth Amendment grounds* – within the past year or so.

The employment context decision, by the Ninth Circuit, was reversed in June 2010 by the U.S. Supreme Court in *City of Ontario v. Quon.*[87] The high court's decision culminated a long cautionary tale as to the importance of maintaining a clear, comprehensive and modernized computer usage policy. The U.S. Supreme did not grant certiorari on the SCA claim against a pager-service provider, instead only addressing the Fourth Amendment claim against the employer itself.

The non-employment decision – in a customer/Internet-Service-Provider (ISP) civil ECPA case – was retracted and then undone by an *en banc* decision by the Sixth Circuit.[88] Once the underlying criminal case was tried, though, in 2011 the Sixth Circuit revisited some of the same concepts on which it had punted in the SCA context in 2007. In *U.S. v. Warshak*,[89] the Sixth Circuit dared to take a stance regarding the reasonable expectation of privacy in, and Fourth Amendment implications of, warrantless searches of email.

Because both the *Quon* and *Warshak* decisions ended up focusing on the respective Fourth Amendment contentions, they are both discussed in detail in the ensuing segment.

---

[86] 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>.

[87] *City of Ontario v. Quon*, 130 S. Ct. 2619 (U.S. June 17, 2010).

[88] *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) ("*Warshak II*") (in face of vehement dissent, vacating preliminary injunction and not addressing SCA issue on grounds of lack of ripeness) <http://www.ca6.uscourts.gov/opinions.pdf/08a0252p-06.pdf>.

[89] *United States v. Warshak*, 631 F.3d 266 (6th Cir. Dec. 14, 2010) <www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf>.

d. Constitutional Limits

i. Fourth Amendment – *Quon, Warshak and Rehberg*

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.[90] The case began in the Central District of California and then progressed to the Ninth Circuit before landing in the Supreme Court.

The key *Quon* defendant – a public sector employer – ultimately succeeded in fending off a Fourth Amendment challenge to enforcement of its Technology Acceptable Use Policy ("TAUP") when it reviewed the contents of a police officer's text messages sent on City-issued pagers. Yet the years of litigation could have been avoided if the employer, the City of Ontario, had been more disciplined in its written policy maintenance and in its policy-enforcement approach.

Quon, along with his fellow officers, signed an acknowledgment of a policy prohibiting personal use of e-mail and warning that employees "should have no expectation of privacy or confidentiality when using [City electronic] resources."[91] However, the pagers were acquired years later, and the City never amended its written policy to encompass personal use of the pagers. Even worse, the Police Department Lieutenant responsible for administering the pager program told Quon and other officers that management would not audit pager use so long as the employee paid for any "overages," *i.e.*, for use exceeding the maximum characters for which the City would pay.[92] Ultimately, Quon paid for overages on several occasions. Later, management obtained Quon's messages and found many personal, sexually explicit messages to his wife and girlfriend.

Upholding Quon's success at trial, the Ninth Circuit held that he had a reasonable expectation of privacy such that the audit of his text messages was unreasonable in scope.[93] The court opined that the Lieutenant's statements *and modus operandi*, combined with Quon's overages payments, effectively did an end-run around the policy. Thus, there was an expectation of privacy for Quon under the Fourth Amendment in his use of the pager to send and receive personal text messages.[94] The Ninth Circuit also upheld the lower court verdict finding that the wireless service had violated the SCA by turning over the messages to the City.

Subsequently, both the employer and the wireless company unsuccessfully sought a panel rehearing; and one of the Ninth Circuit judges called for an *en banc* rehearing. In a split decision, the Ninth Circuit once again agreed with the district court and thus denied both requests. The denial Order specifically noted that the informal pager protocol had established the standard to which the employer was

---

[90] *See Employer Violated Employee Privacy by Accessing Personal Text Messages,* Fenwick Employment Brief (July 10, 2008) <http://www.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.

[91] *Quon*, 529 F.3d at 896, 906 (9th Cir. 2008) ("*Quon I*").

[92] *Id.* at 897, 906-09.

[93] *Id*. at 906-08.

[94] *Id*.

to be held.[95] A vehement dissenting opinion contended that the majority had departed from Supreme Court precedent that had established that the "operational realities of the workplace make some employees' expectations of privacy unreasonable."[96]

The City appealed to the Supreme Court, which reversed the Ninth Circuit[97] by holding that, even assuming a reasonable expectation of privacy, the search was reasonable. In particular, the Court found that the City had a legitimate, work-related rationale for the search and it was not overly intrusive. Quon had not received any guarantees of privacy and thus could have inferred that the City might audit the text messages to monitor work performance. However, the Court declined to opine whether the Fourth Amendment applied in this context, instead indicating: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[98]

Yet, the Court did indicate that, in analyzing the Fourth Amendment's application to government employers, it would likely utilize the two-step approach articulated by the plurality in *O'Connor v. Ortega*, an analogous 1987 Supreme Court workplace privacy case in which the plurality held:

- a court should consider the "operational realities" of the workplace to determine if an employee's constitutional rights are implicated; and
- where an employee has a legitimate privacy expectation, the employer's intrusion upon that expectation should be judged by the standard of reasonableness under all circumstances.[99]

The *Quon* Court's hesitation to expound more fully on the Fourth Amendment vis-à-vis government employers in the context of "emerging technology" means that the law is still unsettled. Yet, of particular interest to all employers is the following statement by the *Quon* Court: "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[100]

---

[95] *Quon v. Arch Wireless Op. Co*., 554 F.3d 769 (9th Cir. Jan. 27, 2009) ("*Quon II)*", also available at <ca9.uscourts.gov/datastore/opinions/2009/02/06/0755282o.pdf>. *But see U.S. v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007) (in criminal prosecution of student/hacker, finding "remote search of computer files on a hard drive by a network administrator was justified under the "special needs" exception to the Fourth Amendment because the administrator reasonably believed the computer had been used to gain unauthorized access to confidential records on a university computer") <ca9.uscourts.gov/datastore/opinions/2007/04/04/0510322.pdf>.

[96] *Quon v. Arch Wireless Operating Co*., 554 F.3d 769 (9th Cir. Jan. 27, 2009) (dissent), also available at <http://www.ca9.uscourts.gov/datastore/opinions/2009/01/27/0755282d.pdf>.

[97] The oral argument transcript is available at <supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf>. *See also* Judy Greenwald, *Policies should be consistent, up to date*, Bus. Ins. Magazine (Apr. 26, 2010) (quoting this White Paper's author) <businessinsurance.com/article/20100425/ISSUE01/304259948>; Laura Davis, *High court goes high tech: Justices to hear employee texting case*, Yahoo! News (Apr. 19, 2010) (also quoting this White Paper's author) <http://news.yahoo.com/s/ynews/ynews_ts1641/print>.

[98] *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629, 177 L.Ed. 2d 216, 78 USLW 4591 (U.S. June 17, 2010).

[99] *O'Connor v. Ortega*, 480 U.S. 709, 718, 725-26 (1987).

[100] 130 S. Ct. at 2630. *See also* Robert D. Brownstone & Sheeva Ghassemi-Vanni, *A Wake-up Call for 21st Century Employers*, D.J. (Sep. 2010) (discussing practical impacts of *Quon*), summarized at <fenwick.com/pressroom/5.1.1.asp?mid=4416&loc=FN> (full copy available on request); Kimberly Atkins, *'Sexting' Case Leaves Privacy Issue Unresolved*, Dolan Media Newswires (6/23/10) (quoting this White Paper's author) <neworleanscitybusiness.com/blog/2010/06/23/sexting-case-leaves-privacy-issue-unresolved/>; Erika Morphy, *SC Leaves Big Questions Open in Text-Message Privacy Case*, TechNewsWorld (6/18/10) (also quoting this White Paper's author) <technewsworld.com/story/70240.html?wlc=1277387484&wlc=1278539561&wlc=1278543468>.

Justice Scalia concurred in part and concurred in the judgment. Scalia expressed his agreement with the Court's ruling, but disappointment in its dicta, especially its tacit endorsement of the *O'Connor* plurality. According to Scalia, the Court refused to articulate a standard for application of the Fourth Amendment and corresponding right of privacy to government employers, but simultaneously provided "a heavy-handed hint about how *they* [lower courts] should proceed."[101] He admonished the Court for hedging its bets by "concocting case-specific standards or issuing opaque opinions …," and added: "[t]he-times-they-are-a-changin' is a feeble excuse for disregard of duty."[102] The Court's hesitation to render a decision about the application of the Fourth Amendment to government employers in the context of "emerging technology" means that the law is still unsettled. However, through the implementation and enforcement of a clear acceptable use policy, a public sector employer can potentially avoid litigation and/or successfully demonstrate the defensibility of its approach.

As to post-*Quon* tips for a privacy-law- compliant TAUP for a public or private employer, *see*:

- *Top Ten Takeaways*
  - 10. CLEAR written policy covering all info. 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 by or costs reimbursed by employer and make the scope clear:
    - in written policy;
    - to all supervisors/managers; and
    - to all staff
  - 8. Specify all employer rights, including to:
    - monitor;
    - search;
    - access;
    - inspect; and
    - read
  - 7. Clear written notice to all employees and covered third parties allowed access
  - 6. Be realistic re: "personal use" – strongly consider "limited" or "incidental" exception 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;
    - conflicts with or harms employer; or
    - harms any 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; *see* Slides 28-31 in Appendix F re:
    - employees' own attorney-client privilege

[101] *Id*. at *38-39.

[102] *Id*. at *38.

        - illicit obtainment or use of Login/PW
- 2. Annual concise reminder notice summarizing key TAUP provisions . . . .
- 1. Periodically – every 2-3 years? – review (and maybe revise) TAUP so it's:
    - consistent with actual practices; and
    - up-to-date as to current technology, *e.g.,* smartphones and social networking sites

In sum, *Quon*'s enduring lessons are: be mindful of what one commits to writing; and erect a divide between one's personal and work-related communications.

The criminal Defendants in *Warshak* were a son, his company, and his mother, who operated a venture that distributed "nutraceuticals," including the male enhancement herbal supplement Enzyte. Defendants were the subject of a criminal indictment containing 112 counts, chief among them money laundering and fraud. Prior to a jury trial, Defendants moved to exclude approximately 27,000 incriminating emails, which the government had obtained by requesting prospective preservation of, and later subpoenaing, email records from Defendants' ISP. The government did not obtain a warrant to establish preservation, or subsequent procurement, of the emails, relying on the Stored Communications Act's provision permitting a "governmental entity" to require a service provider to disclose the contents of electronic communications under certain circumstances. Defendants were convicted on multiple counts.

Ultimately, the appellate court addressed a series of issues that it had considered several years before in a related civil lawsuit brought by Warshak against the federal government. The Sixth Circuit held: "a subscriber enjoys a reasonable expectation of privacy in the contents of emails"[103] sent through an ISP such that the government violates the Fourth Amendment by failing to obtain a warrant in advance of compelling the ISP to relinquish such email records. Yet, the court left open the possibility that an ISP's terms or conditions could alter such reasonable expectation of privacy by indicating an intention to "audit, inspect, and monitor" subscriber email.[104] Further, the court held that the Stored Communications Act is unconstitutional to the extent it permits the government to obtain emails absent a warrant. However, the appellate court did not apply the exclusionary rule and affirmed the trial court's admission into evidence of the 27,000 emails. The Sixth Circuit's rationale was that the government had relied in good faith on the Stored Communications Act to obtain the emails.

Throughout the *Warshak* opinion, the court emphasized the importance of email in daily communication, the highly personal nature of email, and the elevated level of protection email should be afforded. The court noted that email: "is the technological scion of tangible mail, and it plays an indispensable part in the Information Age," and indicated that email should be provided the same level of Fourth Amendment protection as letters and telephone calls: "it would defy common sense to afford emails lesser … protection."[105] Moreover, the court urged: "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[106]

In 2010, in another non-workplace case, the Eleventh Circuit attempted to deal with the question of whether individuals have a privacy right in email – an issue the U.S. Supreme Court has yet to

---

[103] *Id*. at *42-43.

[104] *Id*. at *40-41.

[105] *Id*. at *35-36.

[106] *Id*. at *33.

unambiguously address. The court ultimately declined to establish a definitive precedent, preferring to leave the question open for future decision.

In *Rehberg v. Paulk*,[107] Plaintiff, a citizen, sent anonymous faxes to administrators of a public hospital, criticizing their management and activities. Defendants, the District Attorney and the Chief Investigator at the District Attorney's office, had then investigated Plaintiff's actions as a favor to the hospital. During the investigation, the investigator issued a subpoena to an internet service provider ("ISP") for one of Plaintiff's personal email accounts and obtained emails sent and received from Plaintiff's personal computer. As a result of Defendants' investigation, Plaintiff was indicted on multiple counts of assault and harassment. Eventually, all the charges were ordered dismissed. Plaintiff filed suit against the D.A. and the investigator, alleging, among other allegations, that they invaded his privacy by illegally issuing the subpoena to his ISP. Plaintiff claimed the subpoena had violated his Fourth Amendment right to be free of unreasonable search and seizure.

Rather than decide whether Plaintiff had a reasonable privacy expectation in the contents of his personal emails sent voluntarily through a third-party ISP, the court decided to resolve the case narrowly and leave the privacy issue for another day. Qualified immunity shields government officials who perform discretionary governmental functions from civil liability so long as their conduct does not violate any clearly established constitutional rights. As no precedent had existed defining the bounds of privacy in email, no clearly established constitutional right to privacy existed at the time the investigator had issued the subpoenas. The court thus declined to rule on the greater question of email privacy and instead choose to grant the investigator qualified immunity on Plaintiff's email subpoena claim.

The two non-workplace decisions, in *Warshak III* and *Rehberg*, may impact the standards in similar future employment disputes. In any event, the lesson for individuals, whether in the workplace or otherwise, is that, 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

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.*[108] There, Maricopa County Community College District (the "District") professor Walter Kehowski sent various racially-charged emails to District employees via a District-maintained distribution list. Both the chancellor and the president responded to the incident by publically condemning Kehowski's communications and the underlying racist messages. Students, staff and professors were outraged by the emails and demanded that the District appropriately discipline Kehowski. Although many employees complained that his statements had created a hostile work environment, the District did not discipline Kehowski. The District maintained an anti-harassment policy, but did not invoke it against Kehowski.

A certified class of Hispanic District employees sued the District, its governing board, the chancellor and president for failure to properly respond and discipline Kehowski. The chancellor and president asserted qualified immunity. The Ninth Circuit, with Supreme Court Justice Sandra Day O'Connor sitting by designation, held that Kehowski's speech was protected by the First Amendment and did not constitute unlawful harassment. Furthermore, it reversed the District Court and held that the chancellor and president were entitled to qualified immunity. The court stated: "'There is no categorical "harassment exception" to the First Amendment's free speech.'" *Id*. at 708 (citations omitted). Moreover, it held:

---

[107] *Rehberg v. Paulk*, 611 F.3d 828 (11th Cir. 2010) <http://www.ca11.uscourts.gov/opinions/ops/200911897reh.pdf>.

[108] 605 F.3d 703 (9th Cir. 2009) <www.ca9.uscourts.gov/datastore/opinions/2010/05/20/08-16073.pdf>.

"Harassment law generally targets conduct, and it sweeps in speech as harassment only when consistent with the First Amendment." *Id*. at 710 (citations omitted).

But see Van Heerden v. Bd. of Supervisors of LSU, 2011 WL 5008410 (M.D. La. 10/20/11) (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>.

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

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, including California (*see* individual right of privacy in Cal. Const. Art. 1 §1) and New Jersey (*see Pietrylo*), have enacted more stringent restrictions regarding the interception of wire and electronic communications.[109]

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 Section II(B)(4) below, employers should be aware that, in July 2009, the D.C. Circuit reversed the National Labor Relations Board (the "NLB" or the ""Board"), issuing a decision in a case that, at least in the private sector, touched on the extent to which employers may be able to restrict employees' use of an employer's e-mail system to communicate with each other about union matters.[110] The ultimate decision, by the D.C. Circuit, in that *Register*-Guard case did not globally resolve the pertinent issues, let alone in the many contexts in which disputes can occur. Thus, as to both private and public "union shops," open issues remain as to:

- whether an employer may prohibit all non-business use of its e-mail system; and
- to what extent an employer may monitor employee use of e-mail systems not owned by the employer (*i.e.*, employee use of webmail accounts via a work-provided Internet connection).

Future interpretation of *Register-Guard* in various factual contexts could also have ripple effects in other arenas, whether or not union issues are involved.

---

[109] *See* Brownstone eWorkplace, supra note 2, at 29-30 (.pdf pp. 35-36) <http://White-Paper-8-09-at-35.notlong.com>.

[110] *The Guard Publ'ng Co. d/b/a The Register-Guard and Eugene Newspaper Guild*, 351 NLRB No. 70 (Dec. 16, 2007) <http://www.nlrb.gov/shared_files/Board%20Decisions/351/F35170.pdf >, *reversing in part* and *affirming in part*, Cases 36-CA-8743-1, *et al.* <http://www.nlrb.gov/research/frequently_requested_documents.aspx>. *Cf. AFSCME Local 575 v. PERB; L.A. Cty. Sup. Ct.*, No. B211910 (Cal. App. 2 Dist. 6/10/09) (denying petition re: PERB Dec. No. 1979-C, 32 PERC ¶ 151).

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

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").[111] 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.[112] 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.[113] However, as discussed in detail in this sub-section, there is a split in case law as to the viability of the CFAA's application in cases based on allegations of trade secret misappropriation by a former employee.

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.[114] 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.

Currently on the cutting edge is whether a disloyal employee is an apt defendant on a CFAA cause

---

[111] 18 U.S.C. § 1030.

[112] As to the overall intensification of departing employee's theft of company data, *see generally* Mills, Elinor, *Exiting workers taking confidential data with them*, cNet (Feb. 23, 2009) <http://news.cnet.com/8301-1009_3-10170006-83.html>; CBC News, *Departing workers often steal data from ex-employers: study* (Feb. 23, 2009) (citing Ponemon Institute study) <www.cbc.ca/technology/story/2009/02/23/tech-steal-data.html?ref=rss>.

[113] Ilana S. Rubel, *Screen Grabs*, Daily J. (Mar. 13, 2009), available at <http://www.fenwick.com/docstore/Publications/Litigation/Shrinking_Prospects_CFAA.pdf>.

[114] 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 2008 & Supp. 2010).

of action brought by his/her (former) employer.[115] Employers victimized by disloyal employees have at times successfully found recourse under the CFAA against a worker who appropriated sensitive computer data or sabotaged their employer's computer systems during his/her employment and/or on the way out the door. Since the beginning of 2008 alone, there have been several Circuit court opinions and dozens U.S. district court decisions in this area. The outcomes in those decisions have split roughly evenly. Many of those decisions are compiled and list in Appendix D.

Employers face two main hurdles in establishing their CFAA claims: alleging the requisite lack of authorization; and stating a valid claim for statutorily defined damage and/or loss. 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 the "authorized access" sub-issue has split throughout this decade.[116] 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*.[117] 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.[118]

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.[119] The court thus affirmed the former employee's motion for summary judgment on the CFAA claim against him.

---

[115] Order regarding Motion for Summary Judgment, *Clarity Services, Inc. v. Barney*, Case No. 8:08-cv-T-23TBM (M.D. Fla. February 26, 2010) (where employer "failed to impose any restriction on [employee]'s access to [his] laptop after he resigned and he continued to check his corporate e-mail account after quitting, he did not violate either of the CFAA's "access" requirements even after having returned his work laptop with a scrubbed hard drive) <http://www.theinternetlawgroup.com/pages/download/afd3640c275a3b5249e3f3f8b7a76aac>.

[116] For a detailed discussion of the case-law, *see* Brownstone eWorkplace, supra note 2, at 30-38 (.pdf pp.36-44) <http://White-Paper-8-09-at-36.notlong.com>.

[117] *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>.

[118] *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>.

[119] 581 F.3d at 1135.

In 2010, a number of federal district courts followed *Brekka*.[120] On the other hand, in 2010 and 2011, respectively, two circuit courts – the Fifth and Eleventh also chose not to follow *Brekka* when hearing appeals regarding CFAA criminal prosecutions.[121] Moreover, one 2009 trial court decision within the Tenth Circuit implicitly followed the Seventh Circuit's view as expressed in *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. Mar. 8, 2006), <http://caselaw.findlaw.com/us-7th-circuit/1392048.html>, *on subsequent appeal*, 445 F.3d 749 (7th Cir. July 25, 2006) <http://caselaw.findlaw.com/us-7th-circuit/1115559.html>. In *Statera, Inc. v. Hendricksen*, without written explanation, the U.S. District Court in Colorado issued a temporary restraining order (TRO) based on likelihood of success on the merits of the ex-employer's claims brought under the CFAA and other theories. *See* Ex Parte TRO, 2009 WL 2169235 (D. Colo. July 17, 2009), extended for 60 days by stipulation in TRO, 2009 WL 2358934 (D. Colo. July 20, 2009). Per the eDocket, which has since been sealed, the TRO was again extended by stipulation on September 30, 2009. See TRO, Civil Action No. 09-cv-01684-REB-BNB (D. Colo. Sep. 30, 2009).

In 2010 and 2011, a number of federal district courts followed *Citrin*'s broad view.[122] In addition, in 2011,

---

[120] *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>. *See also* more decisions cited in Richard Raysman and Peter Brown, *Employee 'Unauthorized Access' to Employer Data Under the CFAA*, N.Y.L.J. (Oct. 14, 2010) <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202473343076>. *Cf. State v. Riley*, 412 N.J. Super. 162, 988 A.2d 1252, 1267 (in applying New Jersey's computer crime law, "find[ing] persuasive those decisions that adhere to the narrow interpretation of the federal prohibition of access without or exceeding authorization.") (Oct. 30, 2009) <caselaw.findlaw.com/nj-superior-court/1508996.html>.

[121] *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>.

[122] *Jarosch v. American Family Mutual Insurance Co.*, No. 07-C-0212, 2011 WL 4356346 (E.D. Wis. Sep. 16, 2011) (holding former insurance agents accessed insurance companies' files without authorization because the agents had already planned to start competing business) <http://docs.justia.com/cases/federal/district-courts/wisconsin/wiedce/2:2007cv00212/43000/202/0.pdf >; *Cohen v. Gerson Lehrman Group, Inc.*, No. 09 Civ. 4352 (PKC), 2011 WL 4336683 (S.D.N.Y. Sep. 15, 2011) (denying summary judgment on CFAA claim brought against former employees who modified and deleted data before leaving employment) <http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2009cv04352/345298/165/0.pdf?1316174349>; *Fink v. Time Warner Cable*, --- F.Supp.2d ----, 2011 WL 3962607 (S.D.N.Y. Sep. 7, 2011) (denying motion to dismiss because the changing nature of technology requires a broad reading of access and authorization) <http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2008cv09628/335276/64/0.pdf?1315484558>; *Dental Health Products, Inc. v. Ringo*, No. 08–C–1039, 2011 WL 3793961 (E.D. Wis. Aug. 25, 2011) (granting summary judgment for plaintiff on CFAA claim based on defendant's copying information before leaving employment) <http://docs.justia.com/cases/federal/district-courts/wisconsin/wiedce/1:2008cv01039/48584/155/0.pdf?ts=1314369676>; *Wells Fargo Bank, N.A. v. Clark*, No. CIV. 11-6248-TC, 2011 WL 3715116 (D. Or. Aug. 23, 2011) (granting preliminary injunction for Wells Fargo based on allegations Clark returned his work laptop late and damaged) <http://docs.justia.com/cases/federal/district-courts/oregon/ordce/6:2011cv06248/103693/23/0.pdf?ts=1314190493>; *LKQ Corp. v. Thrasher*, 785 F. Supp. 2d 737 (N.D. Ill. May 23, 2011) (denying dismissal because former employer alleged breach of loyalty by former employee) <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2011cv02743/254901/23/0.pdf?1306234982 >; *Wentworth-Douglas Hosp. v. Young & Novis Prof'l Ass'n*, 2010 WL 3023331, at *3 (D. N.H. July 28, 2010) (denying motion to dismiss; essentially following *Citrin* view by ruling that, under the current version of the CFAA, the "damage and/or transmission" – and not the "access" – is what must be unauthorized) <http://op.bna.com/hl.nsf/id/psts-87uq45/$File/went.pdf>.

a different Ninth Circuit panel (and a split one at that) distinguished and harmonized *Brekka*. *U.S. v. Nosal*, 642 F.3d 781 (9th Cir. Apr. 28, 2011) <ca9.uscourts.gov/datastore/opinions/2011/04/28/10-10038.pdf>, *vacated upon grant of rehearing en banc*, 661 F.3d 1180 (9th Cir. Oct. 27, 2011) <http://www.ca9.uscourts.gov/datastore/opinions/2011/11/02/10-10038o.pdf>. In that criminal case, in the course of reversing the dismissal of an indictment, the appellate court adopted a pro-employer view as to § 1030(e)(6)'s "exceeds authorized access" element. *Id.* at 785-86. Distinguishing the *Brekka* facts, the *Nosal* panel emphasized that the pertinent "computer use policy [had] placed clear and conspicuous restrictions on the employees' access both to the system in general and to the [given] database in particular." *Id.* at 787. *Nosal* is analyzed in Fenwick & West LLP, *Ninth Circuit Holds Computer Fraud and Abuse Act Criminalizes Employee's Access To Information In Violation Of Employer's Express Access Limitations, Lit. Alert* (May 2, 2011) <fenwick.com/docstore/Publications/Litigation/Litigation_Alert_05-02-11.pdf>. *Nosal* had appeared to be a watershed moment for the CFAA, but upon publication of that decision, the Ninth Circuit voted to rehear the case *en banc* and vacate the panel decision. The *en banc* Ninth Circuit court has not issued an opinion in Nosal at the time of this writing.

Some commentators, including this White Paper's author's colleague Sebastian Kaplan, interpret some of the CFAA case law as a third approach that focusing 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 121 above but also a number of district courts that issued decisions in 2011.[123]

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

[123] *Marine Turbo Engineering, Ltd. v. Turbocharger Services Worldwide, LLC*, 2011 WL 6756916 (S.D. Fla. Dec. 22, 2011) (denying motion to dismiss CFAA claim based on violation of employment contract) <http://docs.justia.com/cases/federal/district-courts/florida/flsdce/0:2011cv60621/375992/207/0.pdf?ts=1324644210>; *Farmers Bank & Trust v. Witthuhn*, No. 11-2011-JAR, 2011 WL 4857926 (D. Kan. Oct. 13, 2011) (denying motion to dismiss CFAA claim where reasonable jury could find employer's information security policy could mean defendant exceeded authorized access) <https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2011cv2011-94>; *Seal Source, Inc. v. Calderon*, No. 03:09-CV-00875-HU, 2011 WL 5041275 (D. Or. Sep. 29, 2011) (denying summary judgment for defendant on CFAA claim based on disputed issue whether defendant exceeded his authorized access under his employment contract) <https://ecf.ord.uscourts.gov/doc1/15113896093>, *as adopted* by 2011 WL 5057079 (D. Or. Oct. 24, 2011) <http://docs.justia.com/cases/federal/district-courts/oregon/ordce/3:2009cv00875/93922/102/0.pdf>; *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 10-1029, 2011 WL 4467767 (E.D. Pa. Sep. 23, 2011) (noting lack of contract meant plaintiff could not plead defendant exceeded authorized access) <paed.uscourts.gov/documents/opinions/11D1074P.pdf>; *Facebook, Inc. v. MaxBounty, Inc.*, No. 5:10-cv-04712-JF (HRL), 2011 WL 4346514 (N.D. Cal. Sep. 14, 2011) (denying motion to dismiss CFAA claim based on access to Facebook in violation of Facebook's terms of service) <http://docs.justia.com/cases/federal/district-courts/california/candce/5:2010cv04712/233063/46/0.pdf?1316081987>; *Fontana v. Corry*, No. 10–1685, 2011 WL 4473285 (W.D. Pa. Aug. 30, 2011) (holding plaintiff alleged access exceeding authorization where defendant was granted access to certain accounts, but in fact accessed and transferred money from other accounts) <ecf.pawd.uscourts.gov/doc1/15712879792>, as adopted by 2011 WL 4461313 (Sep. 26, 2011) <docs.justia.com/cases/federal/district-courts/pennsylvania/pawdce/2:2010cv01685/194660/11/0.pdf?ts=1317128656>.

reasonable cost" in a manner that includes any cognizable injury to the complaining party.[124]

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

Exemplary of the stricter approach, in September 2009, two district court decisions each rejected a former employer's "loss" theory, one of them finding as follows:

> allegation of lost revenue as a result of defendant's alleged unfair business competition is not the type of revenue loss contemplated by section 1030(e)(11). The CFAA expressly limits lost profits to revenue lost "because of [an] interruption of service." *See Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004) (concluding that damages under the CFAA are intended to be those related to fixing a computer, and not general profit losses). [Plaintiff] does not allege that it suffered a loss of revenue because their computer functions were inoperative, but because they lost customers as a result of defendants' business activities. This does not constitute loss under the CFAA.

TelQuest Int'l Corp. v. Dedicated Bus. Sys. Inc., 2009 WL 3234226, at *1 (D.N.J. Sep. 30, 2009) <https://ecf.njd.uscourts.gov/doc1/11904233293>. *See also*; *ES&H Inc. v. Allied Safety Consultants, Inc.*, 2009 WL 2996340, at *2-*4 (E.D. Tenn. Sep. 16, 2009) (granting motion to dismiss) <https://ecf.tned.uscourts.gov/doc1/16711323659>.

Similar subsequent decisions have included *Nexsales Corp. v. Salebuild, Inc.*, NO. C-11-3915 EMC, 2012 WL 216260 (N.D. Cal. Jan. 24, 2012) <http://docs.justia.com/cases/federal/district-courts/california/candce/3:2011cv03915/247765/30/0.pdf?1327484476>; *Eagle v. Morgan*, No. CIV.A. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011); *Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio*, No. Civ.A. 09-2751, 2011 WL 6088611 (E.D. Pa. Dec. 7, 2011) <http://docs.justia.com/cases/federal/district-courts/pennsylvania/paedce/2:2009cv02751/308514/54/0.pdf?1323360283>; *Nianni, LLC v. Fox,* No. 2:11-cv-118-FtM-36DNF, 2011 WL 5357820 (M.D. Fla. Nov. 7, 2011) <http://docs.justia.com/cases/federal/district-courts/florida/flmdce/2:2011cv00118/255536/21/0.pdf?1320750756>; *Jarosch v. American Family Mutual*

---

[124] *Wit Walchi Innovation Technologies, GMBH v. Westrick*, NO. 12-CIV-20072, TRO, 2012 WL 33164 (S.D. Fla. Jan. 6, 2012) (holding loss from trade secret misappropriation satisfied statutory requirement) <http://docs.justia.com/cases/federal/district-courts/florida/flsdce/1:2012cv20072/392690/9/0.pdf?ts=1325945305>, as followed in Permanent Injunction Jan. 24, 2012) <http://docs.justia.com/cases/federal/district-courts/florida/flsdce/1:2012cv20072/392690/22/0.pdf?ts=1327495762>; *Garland-Sash v. Lewis*, No. 05 CIV 6827 WHP, 2011 WL 6188712 (S.D.N.Y. Dec. 6, 2011) (holding consequential damages counted toward definition of loss under the CFAA) <https://ecf.nysd.uscourts.gov/doc1/127110050493>; *Executive Sec. Management, Inc. v. Dahl*, No. CV 09-9273 CAS (RCx), 2011 WL 5570140 (C.D. Cal. Nov. 15, 2011) (holding damage to business goodwill constituted a loss under the CFAA) <http://docs.justia.com/cases/federal/district-courts/california/cacdce/2:2009cv09273/461252/165/0.pdf?1321514455>; *Mobile Mark, Inc. v. Pakosz*, No. 11 C 2983, 2011 WL 3898032 (N.D. Ill. Sep. 6, 2011) (holding lost business opportunity constituted loss under the CFAA) <http://www.steptoe.com/assets/attachments/4312.pdf>; *Wells Fargo Bank, N.A. v. Clark*, No. CIV. 11-6248-TC, 2011 WL 3715116 (D. Or. Aug. 23, 2011) (granting preliminary injunction because defendants' threatened disclosure of trade secret information constituted an irreparable injury) <http://docs.justia.com/cases/federal/district-courts/oregon/ordce/6:2011cv06248/103693/23/0.pdf?ts=1314190493>; *Meats by Linz, Inc. v. Dear*, NO. 3:10-CV-1511-D, 2011 WL 1515028 (N.D. Tex. Apr. 20, 2011) (holding lost revenue satisfies CFAA requirement for loss) <http://www.gpo.gov/fdsys/pkg/USCOURTS-txnd-3_10-cv-01511/pdf/USCOURTS-txnd-3_10-cv-01511-0.pdf>.

Insurance Co., No. 07-C-0212, 2011 WL 4356346 (E.D. Wis. Sep. 16, 2011) <http://docs.justia.com/cases/federal/district-courts/wisconsin/wiedce/2:2007cv00212/43000/202/0.pdf >; *Catapult Communics. Corp. v. Foster*, 2010 WL 3023501, at *3 (N.D. Ill. July 30, 2010) ("losses in the form of fees and expenses . . . incurred from conducting forensic analysis" does not constitute the requisite "evidence that [Plaintiff ex-employer's] computers were damaged by Defendant [ex-employee]'s alleged unauthorized access of Plaintiff's files") <http://pub.bna.com/eclr/06cv6112_73010.pdf>; *Consulting Prof'l Resources, Inc. v. Concise Technologies LLC,* 2010 WL 1337723 (W.D. Pa. Mar. 9, 2010) <https://ecf.pawd.uscourts.gov/doc1/15712169362>. *But see Expert Janitorial LLC v. Williams*, 2010 WL 908740, at *2 (E.D. Tenn. Mar. 12, 2010) (denying motion to dismiss where "plaintiff ha[d] alleged that due to [defendants' use of scrubbing software], plaintiff had to institute remedial measures and restore the computer system to the condition it was in prior to the alleged damage") <pub.bna.com/eclr/09cv283_31210.pdf>.

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, an employer recently 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 the *Pulte* case, *see Bombardment Of Employer's Email And Phone Systems States A Claim For Violation Of Computer Fraud And Abuse Act*, Fenwick Employment Brief (Sep. 19, 2011) <http://www.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.

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

---

[125] For a historical overview of the pre-2008 law in this area, *see* Brownstone eWorkplace, supra note 2, at 38-39 (.pdf pp. 44-45) <http://White-Paper-8-09-at-44.notlong.com>.

At the very end of 2007, the since-reversed NLRB issued a split decision in *Register-Guard*,[126] addressing whether private sector employees (such as the newspaper publisher in that case) have the right to use their employer's e-mail system (or other computer-based communication systems) to contact other employees about union or other concerted, protected matters.[127] Each of the majority and dissenting opinions contended that it was being consistent with the Fourth Circuit's *Media General* approach.[128]

The policy at issue prohibited e-mail use "to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations." The Register-Guard, a newspaper, had given two warnings to an employee for sending emails supporting a union. The employee filed an NLRB complaint, alleging that the newspaper's policy was unlawful, in that, in practice, the newspaper allowed employees to send other types of non-work related emails.

The NLRB majority noted that there was no statutory right to use an employer's e-mail system for collective/concerted activity protected under NLRA § 7. The majority then in essence adopted a new standard in assessing the validity of the employer's conduct in the situation at hand. The Board held that:

- "to be unlawful, discrimination must be along Section 7 lines;"
- allowing "nonwork-related" (personal) uses of the e-mail system – such as birth announcements and ticket offers – did not require equal access for union-related solicitations; and
- an employer may forbid union-related communications as long as it also does so regarding similar messages as to other outside *organizations* – such as charities and political causes.

The Board thus tried to render an apples-to-apples comparison of organization-to-organization the new approach to assess whether a policy were enforced in a discriminatory manner vis-à-vis Section 7.

In the summer of 2009, however, the D.C. Circuit reversed the relevant part of the NLRB's *Register-Guard* decision.[129] Unlike the NLRB majority, the circuit court found that the selective enforcement of the e-mail policy's no-solicitation rule *had* been unlawfully discriminatory.[130] Figuring prominently in the

---

[126] *The Guard Publishing Company, d/b/a The Register-Guard*, Cases 36-CA-8743-1, et al. (Feb. 21, 2002) <http://www.nlrb.gov/nlrb/about/foia/documents/J15-02sf.pdf>.

[127] *The Guard Publ'ng Co. d/b/a The Register- Guard and Eugene Newspaper Guild*, 351 NLRB No. 70 (Dec. 16, 2007) <http://www.nlrb.gov/shared_files/Board%20Decisions/351/F35170.pdf >. The NLRB's own detailed summary of its decision – "NLRB FINDS NO STATUTORY RIGHT TO USE EMPLOYER'S E-MAIL SYSTEM FOR 'SECTION 7 COMMUNICATIONS'," Press Release (Dec. 21, 2007) – is at <http://www.nlrb.gov/shared_files/Press%20Releases/2007/R-2652.htm>.

[128] *Media Gen. Operations, Inc. v. NLRB*, 2007 WL 806023, *3, 181 L.R.R.M. (BNA) 2632 (4th Cir. 2007) <http://pacer.ca4.uscourts.gov/opinion.pdf/061023.U.pdf>.

[129] *Guard Publ'g Co. d/b/a Register- Guard v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009) <http://pacer.cadc.uscourts.gov/common/opinions/200907/07-1528-1194980.pdf>. In the public sector, *cf. AFSCME Local 575 v. PERB; L.A. Cty. Sup. Ct.*, No. B211910 (Cal. App. 2 Dist. 6/10/09) (denying petition re: PERB Dec. No. 1979-C, 32 PERC ¶ 151).

[130] *Id.* at 58.

D.C. Circuit's rationale was the fact that the employer had apparently never disciplined any other employee for any e-mail messages other than the e-mails in dispute in the matter at hand.[131]

One key e-mail was union-related but on its face was not a "solicitation," as forbidden by the policy language. That e-mail had not "call[ed] for action" (*i.e.,* had not tried to get employees to join the union); it simply clarified facts as to a rally.[132] Moreover, even though the other key e-mails were indeed solicitations, the pertinent disciplinary warning had never mentioned the organization-versus-individual distinction on which the NLRB had seized "*post hoc*".[133] The express basis the employer had raised for the warning was the union-related content. Thus, the policy – though neutral on its face – had been discriminatorily applied.

As noted in Section II(B)(2) above, the ultimate resolution of the *Register-Guard* issue set seems to have had ripple effects in a variety of arenas.[134] Since the *Register-Guard* appellate decision, the NLRB has begun to address social-media-era TAUP issues. In 2009, an NLRB Regional Director opined that Sears' Holdings' Social Media Policy "d[id] not violate Section 8(a)(1) because it c[ould] not reasonably be interpreted in a way that would chill Section 7 activity."[135]

Last year, an NLRB Complaint in the social-media context resulted in a settlement. Though it did not proceed to adjudication, the case is nonetheless 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 posted negative remarks about her supervisor on her personal Facebook page."[136] "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."[137] After much publicity and speculation in the mainstream media and in the legal press,[138] the matter settled on February 7, 2011.[139] As

---

[131] *Id.* at 60.

[132] *Id.* at 59.

[133] *Id.* at 60.

[134] For pertinent resources generated while the *Register-Guard* appeal was pending, *see* NLRB Office of the General Counsel, *Report on Case Developments* (May 15, 2008) <http://NLRB-GC-5-15-08.notlong.com>. *See also* BNA, Inc., *NLRB General Counsel Issues Report Discussing Recent E-Mail Restriction Cases*, 7 Privacy & Security Law Report No. 21, at 783 (May 26, 2008) <http://7PVLR783-5-26-08.notlong.com> (subscription required); BNA, Inc., *Law Professors at ABA Conference Criticize NLRB Worker E-Mail Ruling*, 7 Privacy & Security Law Report No. 19, at 705 (May 12, 2008) <http://7PVLR705-5-12-08.notlong.com> (subscription required). *See also* Tresa Baldas, *Electronic Message Boards Stir Concerns, Nat'l L. J.* (May 13, 2008) (discussing NLRB Complaint filed in L.A. Regional Office by Cal-Poly student-representatives/employees against Uloop.com) <www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202421318139>; uLoop informal settlement reflected at <http://ULP-NLRB-2008.notlong.com>.

[135] Advice Memorandum, *Sears Holdings (Roebucks)*, No. 18-CA-19081 (Dec. 4, 2009) <http://mynlrb.nlrb.gov/link/document.aspx/09031d45802d802f>.

[136] 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>.

[137] *Id.*

[138] *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>.

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."[140]

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 those recent developments and proceedings tackling whether employee posts constitute employment terms and/or conditions.

Regardless of the gist of *Register-Guard*'s anticipated progeny, 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 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[141]

Employers may wish to prevent misconduct by regularly monitoring their computer systems and network resources.[142] 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.[143] Most decisions regarding the interception of a private employee's e-mail continue to find that no intrusion into the employee's privacy occurred. Yet, it is possible to construct some potentially viable theories of privacy violations.

In early 2008, an invasion of privacy claim was rejected where, "although [an employee] might have believed that he could purchase ['his' employer-provided computer] upon leaving the company, the

---

[139] 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>.

[140] 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>.

[141] *See generally* Brownstone eWorkplace, supra note 2, at 41-44 (.pdf pp. 47-50) <http://White-Paper-8-09-at-47.notlong.com>.

[142] Lynn, Cecil, *Public ESI or Privileged Enforcement of Workplace Computer Privacy Policies*, BNA PSLR (Nov. 17, 2008) (as does this NELI White Paper's author, calling Acceptable Use Policies " 'No Expectation of Privacy' - 'NEoP' - policies") <bna.com/pvln/PVLNWB/split_display.adp?fedfid=11020416&vname=pvlrnotallissues&fcn=19&wsn=505854000&fn=11020416&split=0> (available by subscription); Rozycki, Carla J and Mungerson, Darren M., Enforce Technology-Use Policies to Manage Privacy Conflicts, Law.com (Jan. 30, 3008) <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=900005502067>.

[143] *See* SAMPLES linked from attached Appendix A.

computer was, until that time, [the employer]'s property."[144] Thus, the requisite element of a "highly offensive" intrusion was lacking as a matter of law.[145] An additional factor militating in favor of dismissal was that the former employer "did not look at the computer for the purpose of rooting out personal information about [Plaintiff], but, rather, was motivated by a desire to protect its confidential information and to ensure that [Plaintiff] was not engaged in unauthorized activity that would harm" the company.[146]

The safest method to avoid liability under privacy laws is to achieve prior notice and consent.[147] Employers are wise to disseminate: (1) an employee computer use policy which, at a minimum, puts employees on notice of the employer's right to access its computer files and (2) guidelines for employee use of e-mail.[148] *See* Section V below (and its counterpart in the prior, lengthier white paper) for further discussion of proactive policies.

III. INVESTIGATIONS AND BACKGROUND CHECKS

A. Credit Report Information Under FCRA/FACTA and State-Analogues[149]

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,[150] 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 – already took effect in November 2010; and some others do not take effect until February 2012.[151]

---

[144] *Hilderman v. Enea Teksci, Inc.*, 551 F. Supp. 2d 1183, 1204-1205 (S.D. Cal. 2008) (also dismissing Stored Communications Act claim because e-mails stored on employee's laptop were not encompassed by any of the SCA's threshold definitions).

[145] *Id.* at 1204.

[146] *Id.*

[147] 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).

[148] *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.

[149] For a relatively detailed discussion of this topic, *see* Brownstone eWorkplace, supra note 2, at 44-47 (.pdf pp. 50-53) <http://White-Paper-8-09-at-50.notlong.com>.

[150] 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>.

[151] *See generally* Littler Privacy and Data Protection Practice Group, *Multi-State Employers Must Revise Job Applications to Address New Massachusetts Background Check Law*, workplace Privacy Counsel (Aug. 27, 2010) <http://privacyblog.littler.com/2010/08/articles/background-checks/multistate-employers-must-revise-job-applications-to-address-new-massachusetts-background-check-law/print.html>.

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.[152]

Most notable among the pertinent statutory schemes is the federal Fair Credit Reporting Act ("FCRA"). The FCRA applies to private and public entities alike. Yet many private sector and public sector "employers are unaware of the requirements of the . . . FCRA . . ., 15 U.S.C. § 1681 et seq., which applies to hiring. In fact an even greater number of municipal employers fail to comply with the statute's provisions."[153]

In the private sector, the Obama administration's FTC quickly stepped up FCRA enforcement in this context. In 2009, the FTC succeeded in obtaining FCRA judgments against "[t]wo companies that [had] fired workers and rejected job applicants based on background checks without informing them of their rights under the . . . FCRA."[154]

Since then, 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.[155] 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>. *See generally* the legislative history at <leginfo.ca.gov/cgi-bin/postquery?bill_number=ab_22&sess=CUR&house=B&author=mendoza>; *see also* Rod M. Fliegel and Jennifer L. Mora, *Facing Limits on Background Checks*, Recorder (Sep. 29, 2011) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202517287097>. Many other states have been considering

---

[152] Employers can avoid the application of the Fair Credit Reporting Act ("FCRA") by conducting investigations through "in-house" resources. However, if an employer chooses to proceed using internal resources, it must ensure that the proper steps are taken to accomplish an unbiased and complete investigation.

[153] Governor's Center for Local Government Services, *Model Hiring Manual for Pennsylvania Municipalities*, ch. 1 ("Introduction") – Background Checks, at 5-7 (.pdf pp. 12-14) (Aug. 10, 2004) <http://www.newpa.com/get-local-gov-support/publications/download.aspx?id=324> (hereafter "*Hiring Manual for Pa.*").

[154] FTC, *Two Companies Pay Civil Penalties to Settle FTC Charges; Failed to Give Required Notices to Fired Workers and Rejected Job Applicants*, News Release (Aug. 11, 2009) <ftc.gov/opa/2009/08/qts.shtm>, linking to, *inter alia*, Stipulated Final Judgment and Order, *F.T.C. v. Quality Terminal Services, LLC*, Case No. 09-CV-01853-CMA-BNB, FTC File No. 082 3022 (D. Colo. Aug. 11, 2009) <ftc.gov/os/caselist/0823022/090806qtsstipjdmt.pdf>; Stipulated Final Judgment and Order, *F.T.C. v. Rail Terminal Services, LLC*, Case No. 09-CV-1111, FTC File No. 082 3023 (W.D. Wash. Aug. 11, 2009) <ftc.gov/os/caselist/0823023/090806rtsstipjdmt.pdf>. *See also* Privacy & Security Law Report, *Employers Settle FTC Allegations of Failure To Notify Workers of Credit Report Data Use*, 8 PVLR 1200 (Aug. 17, 2009), available by subscription at <news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=14141453&vname=pvlrnotallissues&fn=14141453&jd=a0b9k0r8f4&split=0>.

[155] *See* Or. SB 1045 <leg.state.or.us/10ss1/measpdf/sb1000.dir/sb1045.en.pdf > (amending Or. Rev. Stats. 659A.885; signed into law on March 29, 2010 by Oregon Governor Kulongoski and effective as of July 2, 2010); Haw. Rev. Stats. § 378-2(8) (amending Hawaiian Fair Employment Practices Act to make it "an unlawful discriminatory practice . . . . [f]or any employer to refuse to hire or employ or to bar or discharge from employment, or otherwise to discriminate against any individual . . . because of the individual's credit history or credit report, unless the information in the individual's credit history or credit report directly relates to a bona fide occupational qualification") <http://www.capitol.hawaii.gov/hrscurrent/Vol07_Ch0346-0398/HRS0378/HRS_0378-0002.htm>; Wash. RCW 19.182.020(2)(c)(i)-(ii) (amendment passed in 2007 banning "consumer report for employment purposes . . . unless the information is either [. . .] [s]ubstantially job related and the employer's reasons for the use of such information are disclosed to the consumer in writing; or [. . .] [r]equired by law") <http://apps.leg.wa.gov/rcw/default.aspx?cite=19.182.020>. *See generally* Andrew Martin, *As a Hiring Filter, Credit Checks Draw Questions* (Apr. 9, 2010) <nytimes.com/2010/04/10/business/10credit.html?pagewanted=print>.

following suit.[156] Moreover, Congress considered, but did not enact, a similar ban, with similar exceptions for when these types of background checks would be permissible.[157]

Lastly, of course using credit checks as to one class of applicants and not others can lead to a Title VII discrimination case. *See, e.g., EEOC v. Kaplan Higher Educ.*, No. 02882 (N.D. Ohio 12/21/10) <http://graphics8.nytimes.com/packages/pdf/KaplanComplaint.pdf >; *partial dismissal* at <http://www.jenner.com/files/tbl_s69NewsDocumentOrder/FileUpload500/9893/Kaplan%20Opinion.pdf >.

B. Legality and Advisability of Following the Internet Trail

Much has been written about the brave new world of Web 2.0 and the quandary it creates for employers considering hiring a given applicant.[158] Painting with a broad brush, some of the emerging principles in this area seem to be as follows:

- Those who post information about themselves on the web without using protections to keep it from being publicly available will have an exceedingly weak "expectation of privacy" argument.[159]
- An employer may lawfully search/Google as to an applicant.[160]
- 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,[161] 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.[162]

---

[156] *See* Joanne Deschenaux, *Maryland, Other States Weigh Limits on Credit Checks for Employment*, SHRM (Mar. 3, 2010) (Connecticut, Georgia, Illinois, Michigan, Missouri, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, South Carolina, Vermont and Wisconsin) <http://www.shrm.org/LegalIssues/StateandLocalResources/Pages/Checks.aspx> (membership may be required to use this URL). *See also* Justin McIntosh, *Credit checks: Ohio proposal would protect workers, job applicants*, Marietta Times (Mar. 3, 2010) ("[s]ixteen states, including Ohio, have proposed outlawing most credit checks for prospective employees") <http://www.mariettatimes.com/page/content.detail/id/519977.html?showlayout=0>.

[157] H.R. 3149 <http://www.govtrack.us/congress/bill.xpd?bill=h111-3149>.

[158] *See, e.g.,* Vickie L. Wallen and Brian Flock, *Social Networking Sites Pose Risk For Employers*, Law 360 (Jan. 28, 2009) <perkinscoie.com/files/upload/WP_09-02_Social_Networking_Sites_Pose_Risk_For_Employers.pdf>; Shari Claire Lewis, *How Private Is Your Social Network?* N.Y.L.J. (Nov. 26, 2008) <law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202426302782> (discussing inconclusive decision in *Corman v. UCG*, 369 F. Supp. 2d 923 (N.D. Ohio 2005) <ecf.ohnd.uscourts.gov/doc1/14102988929>); Ronald J. Levine and Susan L. Swatski-Lebson, *Are Social Networking Sites Discoverable?* Prod. Liab. Law & Strategy (Nov. 13, 2008) <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202425974937>.

[159] *See generally* Jonathan Bick, *Lawful Mining of Blogs on Social Networks*, N.J.L.J. (Feb. 19, 2009) <http://www.bicklaw.com/Publications/LAWFULMININGOFSOCIALNETWORKS.htm> (citing, *inter alia*, *Duran v. Detroit News, Inc.*, 200 Mich. App. 622, 504 N.W. 2d 715 (Mich. Ct. App. 1993).

[160] *Mullins v. Dep't of Commerce*, 244 Fed. Appx. 322, 2007 WL 1302152 (Fed. Cir. May 4, 2007) <http://www.ll.georgetown.edu/FEDERAL/judicial/fed/opinions/06opinions/06-3284.pdf>.

[161] *See* Section IV(D) below.

[162] For a stark example, *see* Molly DiBianca, *Twitter Saves Cisco a Bundle of Money*, Del. Emp. Law Blog (Mar. 30, 2009) <delawareemploymentlawblog.com/2009/03/twitter_saves_cisco_a_bundle_o.html>.

- 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.[163] On the other hand, as at least one employer has publicly announced it is doing, an organization can decide to avoid web research altogether; and some commentators also echo that conservative approach.[164]

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.[165] As noted in Section I(B)(3) above, the FTC recently approved the potential legality of a one-year old start-up company, "Social Intelligence," that does social-media background checks on applicants. In part, Social Intelligence looks into up to seven years of a subject's social-media history, while screening out information that could leave an employer open to legal liability.[166] In sum, the FTC concluded

---

[163] Ben Kerschberg, *Why Corporate Counsel Must Own Social Media Policy*, Forbes (Feb. 1, 2011) <http://blogs.forbes.com/benkerschberg/2011/02/01/why-corporate-counsel-must-own-social-media-policy_consero>; ARMA Int'l, *Employer Policy Urged for Blog Mining*, ARMA Info. Mgmt. NewsWire (Feb. 25, 2009) <http://www.arma.org/news/enewsletters/printFriendly.cfm?id=3445>; Jonathan Bick, *Lawful Mining of Blogs on Social Networks*, N.J.L.J. (Feb. 19, 2009) <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428377614>. *See also* Nancy Hatch Woodward, *Checking up on Applicants via Social Media Sites? Verifying What You Find is Key*, 27 NO. 19 EMPALERT 2 (Sep. 21, 2010), available via subscription at <http://web2.westlaw.com/find/default.wl?rs=WLW11.01&fn=_top&sv=Split&findjuris=00001&mt=208&vr=2.0&rp=%2ffind%2fdefault.wl&cite=27+NO.+19+EMPALERT+2>

[164] Meridith Levinson, *Social Networking Sites Too Risky for Recruiting, Says Bank CEO*, CIO (Apr. 27, 2009) <http://advice.cio.com/meridith_levinson/social_networking_sites_too_risky_for_recruiting_says_bank_ceo>; Jenny B. Davis, *Bank Nixes Use of Social Networking Sites in Hiring Process*, Texas Lawyer (Apr. 13, 2009) <http://www.law.com/jsp/ihc/PubArticleFriendlyIHC.jsp?id=1202429840060>. *See also* Brian Sumers, *Employers looking up job candidates online carry* risk, D.J. (10/12/11), available by subscription at <http://www.dailyjournal.com>; Michelle Sherman, *Social Media Web-Search Pitfalls in Hiring*, Cal. Lawyer (July 2011) <callawyer.com/story.cfm?eid=916593&evid=1> (discussing $125,000 settlement of religious discrimination Title VII claim in *Gaskell v. Univ. of Ky.*, 2010 WL 4867630 (E.D. Ky. 11/23/10) (applicant's alleged creationist views – "MODERN ASTRONOMY, THE BIBLE, AND CREATION" – came to light based on web searching during hiring process for astronomy professor) <media.aclj.org/pdf/gaskell_summary_judgment_order_20101206.pdf>).

[165] Social Intelligence's <http://www.socialintelligencehr.com/> services are discussed in Jennifer Preston, *Social Media History Becomes a New Job Hurdle,* N.Y. Times (July 20, 2011) <http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html>; Leslie Horn, *FTC-Approved Company Will Save Dirt from Your Facebook Profile for 7 Years*, PC Mag. (June 20, 2011) <http://www.pcmag.com/article2/0,2817,2387315,00.asp>. *See also* Alan Farnham, *Background Checks Now Include Twitter, Facebook*, ABC News (June 24, 2011) <http://abcnews.go.com/Business/job-tweets-background-checks-employers-now-include-postings/story?id=13908874>; Kashmir Hill, *Feds Okay Start-up that Monitors Employees' [and applicants'] Internet and Social Media Footprints*, Forbes (6/15/11). <http://blogs.forbes.com/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval>.

[166] The Social Intelligence℠ *"Monitoring" and "Hiring" Solutions* are described at <http://www.socialintelligencehr.com>. *See generally* Leslie Horn, *FTC-Approved Company Will Save Dirt from Your Facebook Profile for 7 Years*, PC Mag. (June 20, 2011) <http://www.pcmag.com/article2/0,2817,2387315,00.asp>. *See also* Alan Farnham, *Background Checks Now Include Twitter, Facebook*, ABC News (June 24, 2011) <http://abcnews.go.com/Business/job-tweets-background-checks-employers-now-include-postings/story?id=13908874>; Kashmir Hill, *Feds Okay Start-up that Monitors Employees' [and applicants'] Internet and Social Media Footprints*, Forbes (June 15, 2011). <http://blogs.forbes.com/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval>.

that, as long as that type of company complies with the Fair Credit Reporting Act ("FCRA"),[167] then it can be a valid "consumer reporting agency."[168]

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*. While such a request would seem to overreach, a recent public sector matter shows the lack of certainty as to the rule of law for this exact scenario.[169]

When the prospective employer is a public entity, even greater care may be necessary.[170] In 2008, the Ninth Circuit ruled that the government may not conduct broad background checks of low-level contract workers who do not work with classified material. In *Nelson v. Nat'l Aeronautics & Space Admin.*,[171] NASA sought to conduct sweeping background checks on low-level contract employees of a private company working at its Jet Propulsion Laboratory. The background checks were part of the application process and governed by a Homeland Security Directive.

The employees sued to stop the background checks from occurring, claiming, among other things, that the checks violated their right to privacy. The court agreed, noting that government intrusions into a person's private matters must be narrowly tailored to achieve a legitimate government interest. While the government's interest in national security was clearly legitimate, it could not show how the broad and highly private searches—which included inquiries into sensitive personal matters such as finances and mental health issues—were narrowly tailored to that interest when the employees were not working on matters directly connected to national security nor exposed to classified material.

Subsequently, however, in January 2011, the U.S. Supreme Court reversed, unanimously finding that there had not been a violation of an informational privacy right.[172] The high Court held that: "In light of the protection provided by the Privacy Act[of 1974]'s nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy."[173] NASA (an agency of the United States Government) had a legitimate interest in conducting basic employment background checks to ensure the security of its facilities and in employing "a competent, reliable workforce."[174] The questions at issue were employment-related inquiries that furthered the NASA's

---

[167] *See generally* Section III(A) supra.

[168] FTC, *RE: Social Intelligence Corp.* (May 9, 2011) <ftc.gov/os/closings/110509socialintelligenceletter.pdf>. *See also* <http://www.reputation.com/> and <http://www.parasec.com/>.

[169] *See* Gordon supra notes 62 and 85 above (raising argument that applicant's consent could arguably distinguish the *Pietrylo*-type situation discussed in Section II(A)(1)(c) above.

[170] *See* Fenwick & West LLP, *Unnecessarily Broad Background Checks Halted As an Invasion of Privacy*, Emp. Brief (Feb. 8, 2008) (discussing the now-vacated *Nelson* Ninth Circuit decision) <fenwick.com/publications/6.5.4.asp?mid=31#nb>, from which part of the ensuing discussion is adapted.

[171] *Nelson v. National Aeronautics and Space Admin. (NASA)*, 530 F.3d 865 (9th Cir. 2008) <ca9.uscourts.gov/datastore/opinions/2008/06/19/0756424.pdf>, *reversed* , 131 S. Ct. 746, 79 USLW 4043 (Jan. 19, 2011) <http://www.supremecourt.gov/opinions/10pdf/09-530.pdf>.

[172] *National Aeronautics and Space Admin. (NASA) v. Nelson*, 131 S. Ct. 746, 79 USLW 4043 (Jan. 19, 2011) <http://www.supremecourt.gov/opinions/10pdf/09-530.pdf>.

[173] *Id.* at 763-64.

interests in managing its internal operations. The mere fact that the statutory non-disclosure requirement is subject to exceptions did not undermine the protections provided.[175]

The *Nelson* case's setting is focused on background searches conducted by a government agency.[176] Nonetheless, private sector employers should also remain mindful of the privacy protections offered by federal and state law and carefully consider the appropriate breadth of proposed background checks.[177]

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.[178] As to public employers, in 2009 a federal district court decision rejected a middle school principal's common law and SCA claims against her former supervisor, the local superintendent of schools.[179] Significantly, however, the same decision denied summary judgment on her Fourth Amendment claim.[180] Moreover, as discussed above regarding *Quon I*,[181] the Fourth Amendment may be implicated by physical searches as well as by searches for electronically stored information such as text messages.

Note also that the Fourth Amendment protection afforded text messages was further contracted in early 2011 by the Supreme Court of California in *People v. Diaz*, in the context of a search incident to a lawful arrest.[182] There, a deputy sheriff witnessed Diaz participate in the sale of narcotics to a police informant. Once

---

[174] *Id.* at 758.

[175] *Id.* at 762.

[176] Note the post-9/11 applicability to employees of federal government contractors as well. *See generally* Adam Liptak, *Justices Uphold Background Checks*, N.Y. Times (Jan. 19, 2011) <http://www.nytimes.com/2011/01/20/us/20scotus.html>.

[177] The *Nelson* court found that an employer's entitlement to a safe, efficient, and effective workforce makes it reasonable to inquire into employees' prior illegal drug use. Courtney Ross Samford, *NASA v. Nelson: Do Employees Have Informational Privacy?* Wyatt Employment Law Report (Feb. 3, 2011) <wyattemployment.wordpress.com/2011/02/03/nasa-v-nelson-do-employees-have-informational-privacy/>. But it is not clear how an employer performing such background checks would avoid violating ADA protection of employees with a history of substance abuse. "For example, the Court recognized that inquiry into an employee's prior illegal drug use is reasonable because all employers are entitled to have a reliable, efficient, and effective workforce." *Id.*

[178] *See* Brownstone eWorkplace, supra note 2, at 49-50 (.pdf pp. 55-56) <http://White-Paper-8-09-at-55.notlong.com>.

[179] *Brown-Criscuolo v. Wolfe*, 601 F. Supp. 2d 441 (D. Conn. 2009) <ecf.ctd.uscourts.gov/doc1/04102051731>.

[180] *Id. But see United States v. Larson*, 66 M.J. 212 (U.S. Armed Forces Apr. 25, 2008) (distinguishing the *Long* banner-warnings case discussed below) <armfor.uscourts.gov/opinions/2008Term/07-0263.pdf>.

[181] *See* notes 95-96 and accompanying text above as to conflicting standards debated by the Ninth Circuit.

[182] *People v. Diaz*, 51 Cal. 4th 84, 244 P.3d 501 (2011) <epic.org/privacy/devicesearch/People_v_Diaz.pdf>.

the sale was completed, the deputy stopped Diaz and arrested him for conspiracy in the sale of drugs. Incident to his arrest, the deputy conducted a search of Diaz's person and found drugs and his cell phone.

Upon arriving at the station, the deputy questioned Diaz to no avail. A full one and one half hours after arresting Diaz, the deputy searched Diaz's cell phone and found an incriminating text message. Once confronted with the text message, Diaz admitted to participating in the drug deal. Diaz later moved to suppress both the text message and his subsequent confession as fruits of an unlawful, warrantless search. The California high court affirmed the decisions of the appellate and lower courts, finding that the search was a lawful search incident to arrest because the cell phone was "'immediately associated with [Diaz's] person' at the time of arrest,"[183] which is an exception to the Fourth Amendment's warrant requirement.

The court did not seem to be overly concerned with the impact of developments in "modern technology" on searches incident to a lawful arrest, indicating: "If … the wisdom of the high court's decisions 'must be newly evaluated' in light of modern technology … then that reevaluation must be undertaken by the high court itself."[184] Moreover, the court echoed previous U.S. Supreme Court search and seizure cases, such as *United States v. Ross*,[185] in articulating that the character of the searched item should not influence the analysis of whether a warrantless search was lawful, despite the seemingly infinite storage capacity of cell phones. The *Diaz* court noted: "differing expectations of privacy based on the amount of information a particular item contains should … be irrelevant."[186]

2. Personal Searches

Personal searches are more intrusive than work area searches and therefore can only be justified by an employer's strong showing of need. Employers should avoid conducting personal searches unless they can demonstrate 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. Thus, in *United States v. Gonzalez*,[187] the Ninth Circuit upheld a random search of an employee's backpack by a store security guard in large part because the employee was aware of the employer's policy that it would conduct random searches.[188] The court concluded that the employer was entitled to search the employee's backpack for stolen merchandise only because the employee had clear notice beforehand that he would be subject to just such a search. As an important instructive point to employers, the court noted that "an employee on his first day who had not yet signed or learned of the store policy might be in a much stronger position to have a reasonable expectation of privacy deserving protection from such searches."188F[189]

---

[183] *Id*. at 93.

[184] *Id*. at 101.

[185] *United States v. Ross*, 456 U.S. 798 (1982) <http://www.law.cornell.edu/supct/html/historics/USSC_CR_0456_0798_ZS.html>.

[186] *Id*. at 97.

[187] *United States v. Gonzalez*, 300 F.3d 1048 (9th Cir. 2002).

[188] *Id*. at 1055.

[189] *Id*.

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

Video surveillance may help deter employee misconduct, including theft and drug use. The author is unaware of any federal or state statute expressly regulating an employer's right to use video surveillance, at least in the private sector.[190] At least one federal circuit held, a number of years ago, that the ECPA does not encompass video surveillance where the recording does not capture audio.[191] 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.[192]

In 2009, the California Supreme Court revisited in great detail the issues it had addressed a decade earlier in *Sanders v. American Broadcasting Companies*, 20 Cal. 4th 907 (1999).[193] This newer case, *Hernandez v. Hillsides*, dealt with a private sector employer. However, in light of California's constitutional right of privacy, the court made clear that it was addressing some issues that arise as to both common-law and California-constitutional-law invasion-of-privacy causes of actions.[194]

In *Hernandez*, in a seemingly unique factual context, the court found the circumstances of an employer's targeted videotape surveillance to meet one key element of an invasion claim but to fall short as to another key element. In sum, though there was an intrusion on two employees' reasonable expectation of privacy, the intrusion was not sufficiently offensive or serious to give rise to liability.[195] The *Hernandez* facts involved a private nonprofit residential facility for neglected and abused children. Especially because some of the children had been victims of sexual abuse, the employer became very concerned when it discovered that, "late at night, after plaintiffs had left the premises, an unknown person had repeatedly used a computer in [the two] plaintiffs' office to access the Internet and view pornographic Web sites."[196] Hoping to catch the culprit, the employer set up a hidden video camera in the office shared by the two co-workers. The remotely operated camera was set up to record and/or enable live viewing only after-hours.

---

[190] Video surveillance by public employers may violate the Fourth Amendment, but only when the recording targets areas in which employees have a reasonable expectation of privacy. *See Vega-Rodriguez v. Puerto Rico Tel. Co.*, 110 F3d 174 (1st Cir. 1997).

[191] *Thompson v. Johnson County Cmty. Coll.*, 1997 U.S. App. LEXIS 5832 (10th Cir. 1997) (unpublished).

[192] *See* Brownstone eWorkplace, supra note 2, at 51 (.pdf p. 57) <http://White-Paper-8-09.notlong.com>.

[193] *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 211 P.3d 1063, 97 Cal. Rptr. 3d 274 (2009) <http://www.courtinfo.ca.gov/opinions/archive/S147552.PDF>. For analysis published both just after and just before this decision came down, *see* Oncidi, Anthony J. and Gross, David, *Here's Looking at You*, L.A. & S.F. Daily J. (July 17, 2009); McKee, Mike, *State Supreme Court Narrows Workplace Privacy*, Recorder (Aug. 4, 2009) <http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202432777025>; Ernde, Laura, *Court Allows Hidden Cameras In Workplace*, L.A. & S.F. Daily J. (Aug. 4, 2009); Ferrari, Anna and Lyon, Christine, *Workplace Video Surveillance: New Guidance from the California Supreme Court*, BNA PLSR (Aug. 10, 2009), available by subscription at <http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=14125478&vname=pvlrnotallissues&fn=14125478&jd=a0b9g5e2k9&split=0>

[194] *Id.* at 286.

[195] *Id.* at 295.

[196] *Id.* at 277.

After the two co-workers discovered the hidden camera, they sued their employer and the facility's Director for privacy-invasion and other causes of action. The trial court granted summary judgment for Defendants; but the intermediate appellate court reversed. Review was granted by the Supreme Court of California.

The parties had agreed "that the camera was not operated for either of the [intended] purposes during business hours, and, as a consequence, that plaintiffs' activities in the office were not viewed or recorded by means of the surveillance system."[197] Defendant Director "did not expect or intend to catch plaintiffs on tape."[198] Based in large part on those facts, the California Supreme Court agreed with the trial court that summary judgment was warranted. But in so ruling, the high court, as noted above, reached divergent conclusions as to the "reasonable privacy expectations" and "highly offensive intrusion" elements.

It remains to be seen whether – and, if so, to what extent, *Hernandez* will affect invasion case-law. Moreover, no Fourth Amendment concerns were implicated in the *Hernandez* scenario, in part because Plaintiffs were neither suspects nor investigative targets. 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.[199] States such as California have statutes outright prohibiting videotaping in certain locations.[200] For those failing to observe such basic decency, liability awaits: Sheraton Hotels paid $200,000 to settle invasion of privacy claims filed by employees covertly videotaped in changing areas.

In the wake of *Hernandez*, on October 20, 2009 a rail labor union sued in federal and state court, seeking to enjoin a plan that the Complaint describes 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."[201] Those video-tapings were intended to catch train engineers in the act of 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

---

[197] *Id.*

[198] *Id.*

[199] *See Koeppel v. Speirs*, 779 N.W.2d 494 (Iowa Ct. App. 2010), unpublished decision at *Koeppel v. Speirs*, 2010 Iowa App. LEXIS 25 (Iowa Ct. App. Jan. 22, 2010) (following *Hernandez* by finding an actual intrusion upon privacy where employer installed surveillance camera in office bathroom; even though camera not operational at time of discovery by police, simply plugging equipment into electrical outlet could have rendered it operational) <http://www.iowacourts.gov/court_of_appeals/Recent_Opinions/20100122/9-902.pdf>.

[200] *See, e.g.,* Cal. Labor Code § 435(a) ("No employer may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes, unless authorized by court order") <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=lab&group=00001-01000&file=430-435>; Cal. Penal Code § 647(j)(1) (prohibiting "look[ing]s through a hole or opening, into, or otherwise views, by means of any instrumentality, including, but not limited to, a periscope, telescope, binoculars, camera, motion picture camera, or camcorder, the interior of a bedroom, bathroom, changing room, fitting room, dressing room, or tanning booth, or the interior of any other area in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy of a person or persons inside") <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=639-653.2>; Cal. Penal Code § 653n ("[a]ny person who installs or who maintains . . . any two-way mirror permitting observation of any restroom, toilet, bathroom, washroom, shower, locker room, fitting room, motel room, or hotel room, is guilty of a misdemeanor") <www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=639-653.2>.

[201] *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 available at <https://ecf.cacd.uscourts.gov/cgi-bin/DktRpt.pl?588578789685931-L_674_0-1>. *See also* Kate Moser, *Railroad Workers Sue Over Privacy at Work* (Recorder Oct. 22, 2009) <law.com/jsp/ca/PubArticleCA.jsp?id=1202434841437>.

use of their laptops.[202] Subsequently, the court granted a Motion for Judgment on the Pleadings, which is now on appeal to the Ninth Circuit.[203]

In the past couple 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. *See, e.g.*, Will Kane, Safety board: Ban Cell Phones For Truckers, S.F. Chronicle (October 14, 2011) <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/10/14/MN831LHA52.DTL&type=printable >; NTSB, Safety recommendation H-11-29, H-06-28 [Reclassification] (Oct. 4, 2011) (urging all states and D.C. to take action) <http://www.ntsb.gov/doclib/recletters/2011/H-11-029.pdf>; NTSB Office of Public Affairs, *NTSB calls for ban on use of mobile phones by commercial drivers; cites need for improved mediam [sic] barriers in accident that killed 11 in Kentucky*, Press release (Sep. 13, 2011) <http://www.ntsb.gov/news/2011/110913.html>; D.O.T., *U.S. Transp. Sec'y Ray LaHood Proposes Rule to Ban Texting for Truck & Bus Drivers*, DOT 55-10 (Mar. 31, 2010) <dot.gov/affairs/2010/dot5510.htm>; Richtel, Matt, *Texting While Driving Banned for Fed. Staff*, NYT (Oct. 2, 2009) <nytimes.com/2009/10/02/technology/02distracted.html?pagewanted=print>; Exec. Order, *FEDERAL LEADERSHIP ON REDUCING TEXT MESSAGING WHILE DRIVING* (Oct. 1, 2009) <whitehouse.gov/the_press_office/Executive-Order-Federal-Leadership-on-Reducing-Text-Messaging-while-Driving/>. *See also* Larry Copeland, *Software Aims To Block Texting While Driving*, NewsFactor (July 22, 2010) <http://www.newsfactor.com/story.xhtml?story_id=74411>.

As with most forms of monitoring, employers should also consider implementing a written policy that provides employees with advance notice that they may be subject to video surveillance.[204] Moreover, as alleged in the Metrolink cases, video surveillance may be a mandatory bargaining subject in union shops.[205]

C. GPS Tracking – including RFID and GPS[206]

Some employers have adopted monitoring technologies to help track employee productivity and movement, including Radio Frequency Identification Systems ("RFID") and Global Positioning Systems ("GPS"). Uses of RFID and GPS vary widely, from simple key-card electronic access employed in many workplaces to more advanced systems that can track an employee's precise location nearly anywhere on the planet.

Employers who currently use GPS technology are in the minority, with only 3 percent using GPS to monitor cell phones;[207] 8 percent using GPS to track company vehicles;[208] and less than 1% percent using

---

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

[203] Civil Minutes, *Bhd. of Locomotive Eng'rs & Trainmen, et al. v. S. Cal. Reg'l Rail Auth.*, CV 09-8286 PA (JEMx) (C.D. Cal. June 30, 2010) <https://ecf.cacd.uscourts.gov/doc1/031110444467>.

[204] See *Clement v. Sheraton Boston Corp.*, 1 Mass. L. Rep. 579, 1993 Mass. Super. LEXIS 314 (Mass. Super. Ct. 1993) (discussing other legal issues prior to settlement).

[205] *See generally* Norman Brand (editor), *Discipline & Discharge in Arbitration*, Ch. 13, § XI(B)(2), *External Law – Monitoring – Surveillance* (BNA 2008) <storefront.bnabooks.com/epages/bnastore.sf/seccx5_5FmWxAc/?ObjectPath=/Shops/bnastore/Products/1555>; *See generally* Elkouri & Elkouri (Alan Miles Ruben, editor-in-chief), *How Arbitration Works*, Ch. 8, § 4(F)(7)(I)(i) (*Evidence – Arbitrator Consultation of Experts – Search of an Employee's Person or Property – Surveillance of Employees* (BNA 2003 & Supp. 2008) <storefront.bnabooks.com/epages/bnastore.sf/en_US/?ObjectPath=/Shops/bnastore/Products/9592>.

[206] To learn more about this topic, *see* Brownstone eWorkplace, supra note 2, at 53-55 (.pdf pp. 59-61) <http://white-paper-8-09-at-59.notlong.com>.

[207] American Management Association (AMA), *The Latest on Workplace Monitoring and Surveillance*, 3 Moving Ahead Newsletter No. 4 (Apr. 2008) <http://www.amanet.org/movingahead/editorial.cfm?Ed=697>.

GPS to monitor employee ID/Smartcards.[209]

The majority of companies using RFID employ Smartcard technology to control physical security and access to buildings and data centers.[210] But physical implantation of RFID chips into an employee is, of course, a wholly different matter. Note that at least four states' statutes expressly prohibit compulsory implantation of RFID chips.[211]

Even where employers have a legitimate reason to use such technologies, there is a risk of misinterpreting GPS information and/or linking it to other personally identifiable information. Moreover, RFID tracking could trigger issues under the NLRA and/or the Fair Labor Standards Act (FLSA).[212]

In contrast to the present technological viability for RFID and GPS monitoring,[213] biometric identification tools are not yet viable, at least on a widespread level.

D. "Off-Duty" Activities

As discussed above, employers wishing to monitor and control their employees' on-duty activities face a number of restrictions and potential sources of liability. In most instances, employers will encounter even more rigorous restrictions when they seek to control employees' conduct away from work.

Employers urge that they have a number of legitimate interests that justify their regulation of employees' off-duty conduct, ranging from preventing conflicts of interest, such as prohibitions on moonlighting for a direct competitor, to policies intended to prevent sexual harassment claims, such as anti-fraternization rules. Employers also legitimately take issue with employees' off-duty conduct that portrays the company in a negative light or causes an actual business loss.

On the other hand, employees understandably have a higher expectation of privacy for off-the-job conduct, as recognized by state statutes: thirty states and the District of Columbia have some form of

---

[208] *Id.*

[209] *Id.*

[210] *Id. Cf.* Dave Bailey, *EU warns firms on RFID tags*, Computing.Co.UK (May 12, 2009) ("EU Commissioner Viviane Reding heads off any attempts to track consumers and their preferences using RFID tags") <http://www.computing.co.uk/articles/print/2242126>.

[211] Keene II, David R., *Subcutaneous RFID Tag Implants - 'Beam Me Up, Scotty,'* Lorman HRResource (July 10, 2008) <http://www.hrresource.com/blog/view.php?blog_id=420>.

[212] *See* Nan Netherton, *Workplace Surveillance, RFID Reviewed at ABA Workplace Technology Meeting*, 8 PVLR 712 (May 11, 2009) <news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=12369232&vname=pvlrnotallissues&fn=12369232&jd=a0b8q7t3u9&split=0>.

[213] For some fairly recent resources on location –tracking, *see* Seth Schoen, *What Location Tracking Looks Like*, EFF Deeplinks Blog (Mar. 29, 2011) </www.eff.org/deeplinks/2011/03/what-location-tracking-looks>; Noam Cohen, *It's Tracking Your Every Move & You May Not Even Know*, NYT (Mar. 26, 2011) <www.nytimes.com/2011/03/26/business/media/26privacy.html>; ACLUNC dotrights, *Location-Based Services Privacy Check-In* (Nov. 16, 2010) <dotrights.org/sites/default/files/lbs-comparison.pdf>; ACLUNC dotrights, Location-Based Services: Time for a Privacy Check-In (Oct. 25, 2010) <http://dotrights.org/sites/default/files/lbs-white-paper.pdf>.

statutory protection for employees' off-duty conduct, and that number increases when one includes states that regulate this area through common law privacy protections.[214]

In addressing whether an employer may legitimately restrict or sanction employees' off-duty conduct, courts will generally consider the extent to which the at-issue conduct affects the employee's ability to perform their job. While courts will tolerate company policies prohibiting employees from engaging in detrimental activities with a clear nexus to the workplace, they will not tolerate employers that discipline employees for legal off-duty conduct that bears no relationship to their employment.

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* Brownstone eWorkplace, supra note 2, at 56-57 (.pdf pp. 62-63) <http://White-Paper-8-09-at-62.notlong.com>.

2. Substance Use

For a relatively detailed discussion of this second area, *see* Brownstone eWorkplace, supra note 2, at 57-59 (.pdf pp. 63-65) <http://White-Paper-8-09-at-63.notlong.com>.

A relatively recent variation on a theme: a Tennessee employer embroiled in multiple ADA proceedings – one brought by employees and one by the EEOC – based on allegedly illegal testing for prescription drugs.[215] The EEOC case is still pending, with a jury trial scheduled for June 5, 2012; but six of the seven private-plaintiffs/employees obtained a successful jury verdict on their ADA claims.[216]

3. Dating and Intimate Relationships

Because intimate relationships fall within the most zealously protected areas of privacy law, employers seeking to regulate their employees' romantic lives should exercise due caution and carefully explore whether the contemplated restriction can truly be justified by business needs. That said, over time policies restricting office romance implemented in an effort to prevent sexual harassment claims have been upheld.[217]

---

[214] *See, e.g.,* Molly DiBianca, *Terminating Employees for Off-Duty Conduct*, Del. Emp. Law Blog (Oct. 20, 2008) <delawareemploymentlawblog.com/2008/10/terminating_employees_for_offd_3.html>.

[215] *See Bates et al v. Dura Automotive Systems, Inc.*, Case No. 1:08-cv-00029 (M.D. Tenn. May 28, 2009) (class action), eDocket available at <https://ecf.tnmd.uscourts.gov/cgi-bin/DktRpt.pl?463097226664399-L_673_0-1>; *EEOC v. Dura Automotive Systems, Inc.*, Case No. 1:09-cv-00059 (M.D. Tenn. Sep. 11, 2009), eDocket available at <https://ecf.tnmd.uscourts.gov/cgi-bin/DktRpt.pl?369597106580365-L_673_0-1> *See also* U.S. EEOC, *EEOC SUES DURA AUTOMOTIVE SYSTEMS FOR VIOLATIONS OF AMERICANS WITH DISABILITIES ACT*, News Release (Sep. 14, 2009) <www.eeoc.gov/press/9-14-09e.html>. *See also* Tresa Baldas, *Employer Sued Twice Over Drug Testing*, Nat'l L.J. (Sep. 24, 2009) <www.law.com/jsp/ca/PubArticleCA.jsp?id=1202434027065>.

[216] For the latest on the *EEOC v. Dura* case, *see* the eDocket at <https://ecf.tnmd.uscourts.gov/cgi-bin/DktRpt.pl?739841050368523-L_674_0-1>. For the Judgment in the private *Bates* action, see JUDGMENT IN A CIVIL CASE (July 26, 2011) <https://ecf.tnmd.uscourts.gov/doc1/16911687911>.

[217] Brownstone eWorkplace, supra note 2, at 59-60 (.pdf pp. 65-66) <http://White-Paper-8-09-at-65.notlong.com>.

In 2008, the Seventh Circuit Court of Appeals rejected a former manager's claims that UPS discriminated against him under Title VII because he was involved in an interracial relationship. In *Ellis v. United Parcel Service*,[218] UPS maintained a non-fraternization policy that prohibited managers from dating hourly employees. Fully aware of the policy, Gerald Ellis, an African-American UPS manager, secretly dated a Caucasian hourly employee. After three years, management learned about the relationship, and warned Ellis that he was violating UPS's non-fraternization policy and needed to "rectify the situation." But Ellis continued the relationship; in fact, the couple got engaged three days later and married a year thereafter.

When management learned of the ongoing relationship, UPS fired Ellis for violating the policy and for dishonesty. Without deciding whether an employee may sue for discrimination under Title VII based on interracial dating, the court rejected Ellis's discrimination claim, based in part on evidence that UPS treated a manager in a same-race relationship similarly and on the fact that Ellis offered no evidence to challenge UPS's legitimate business reasons for his termination – violation of company policy and dishonesty.

Central to UPS's success in *Ellis* was its past consistent enforcement of the non-fraternization policy, and the early involvement of HR in the disciplinary process. Similarly, also in 2008, Wal-Mart's dismissal of an employee for admittedly violating a non-fraternization policy was upheld by an Arkansas appellate court. [219] There, the employer had gone to the extreme measures of having a private investigator follow a couple – a manager and his subordinate – to Guatemala.

Of course, when a case involves an intimate relationship with a minor, many other concerns are raised. For example, in late 2008, a Delaware appellate court upheld the termination of a school teacher, in light of the immorality of his sexual affair with a 17 year old girl he had taught when she was in elementary school.[220] In 2011, in a situation that could have broader impact, the Missouri legislature passed a set of Missouri state statutes <colecountycourts.org/Missouri%20State%20Teachers%20vs%20Missouri.pdf> seeking to restrict Internet contact between teachers and students of high school age and younger. Immediately, the state's teachers sued to challenge the legality of the enactments, "the Amy Hestir Student Protection Act," (SB 54), on constitutional and other grounds. *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>. A preliminary injunction promptly ensued <colecountycourts.org/Missouri%20State%20Teachers%20vs%20Missouri.pdf>; but the case is still pending. *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>.

---

[218] *Ellis v. UPS*, 523 F.3d 823 (7th Cir. 2008) <caselaw.findlaw.com/us-7th-circuit/1386072.html>. *See* Fenwick & West, *Manager Fired For Violating Policy, not Interracial Relationship*, Emp. Brief (May 15, 2008) <fenwick.com/publications/6.5.4.asp?mid=34#manager>, from which the ensuing discussion was adapted.

[219] *Lynn v. Wal-Mart Stores, Inc.*, 280 S.W.3d 574 (Ark. App. Mar. 19, 2008) <http://courts.arkansas.gov/opinions/2008a/20080319/ca07-384.pdf>. *See generally* Molly DiBianca, *Employers' [Private] Eyes Are Watching You*, Del. Emp. Law Blog (May 20, 2008) <delawareemploymentlawblog.com/2008/05/employers_private_eyes_are_wat.html?action=print>.

[220] *Lehto v. Bd. of Educ. of the Caesar Rodney Sch. Dist.*, 962 A.2d 222 (Del. 2008) <http://courts.state.de.us/opinions/(a4sdynji0why1t55z0gv2v45)/download.aspx?ID=114560>; *See generally* Sheldon N. Sandler, *Delaware Decision on Teacher's "Immorality" Has Implications for Employers* (Dec. 9, 2008) <www.delawareemploymentlawblog.com/2008/12/delaware_decision_on_teachers.html?action=print>.

4. Arrests and Convictions

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.[221]

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. While a few states expressly prohibit use of arrest and conviction records in employment decisions, most statutes include at least some type of exception. For example, the Wisconsin Fair Employment Act[222] prohibits employers from discriminating against an employee on the basis of the employee's arrest record or criminal conviction. The Act makes an exception to its general prohibition against discrimination based on arrest and conviction record when an employer can show that the circumstances of an individual's arrest or conviction "substantially relate to the circumstances of the particular job."[223]

In late 2008, Starbucks defeated a class action arising out of the criminal background question in its job application.[224] The application asked: "Have you been convicted of a crime in the last seven (7) years? If Yes, list convictions that are a matter of public records (arrests are not convictions). A conviction will not necessarily disqualify you for employment." On a separate page, the application contained disclaimers for various states, including one for California, which provided: "CALIFORNIA APPLICANTS ONLY: Applicant may omit any convictions for the possession of marijuana (except for convictions for the possessions of marijuana on school grounds or possession of concentrated cannabis) that are more than two (2) years old, and any information concerning a referral to, and participation in, any pretrial or post trial diversion program."

Plaintiffs, a group of rejected applicants, alleged that the criminal history question was unlawful. A California court of appeal found that the disclaimer was lawful, but that its placement on the application was troubling.[225] Had Starbucks included the California disclaimer immediately following the convictions question, the court would have upheld the dismissal of the lawsuit on that ground alone. Instead, the court dismissed the lawsuit on the grounds that, of the four plaintiffs, two admitted in discovery that they understood Starbucks was not seeking information about proscribed marijuana-related offenses, and none had any marijuana-related convictions to disclose.[226] The court may have ruled differently had one or more of the applicants possessed a different understanding and/or disclosed such convictions because of confusion over the form.

---

[221] *See, e.g.,* Tresa Baldas, *Everybody's thinking criminal records check after Michael Vick*, Nat'l L.J. (Aug. 12, 2009) <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202433006044>.

[222] Wis. Stat. § 111.321.

[223] Wis. Stat. § 111.335(1)(b).

[224] *See generally* Fenwick & West, *Starbucks Prevails in Claim of Unlawful Criminal History Question in Application*, Emp. Brief (Jan. 13, 2009), from which the ensuing discussion was adapted <http://www.fenwick.com/publications/6.5.4.asp?mid=42#starbucks>.

[225] *Starbucks Corp. v. Superior Court*, 168 Cal. App. 4th 1436, 86 Cal. Rptr. 3d 482 (2008) <http://www.courtinfo.ca.gov/opinions/archive/G039700.PDF>.

[226] *Id.*

Employers are urged to compare their application language regarding convictions with that approved by the court, and to place the disclaimer on the same page as the conviction inquiry.

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.[227] As discussed above regarding prospects, well-thought out policies and consistent application thereof can greatly help an employer develop a legally defensible approach. Following are some of the scenarios that have come to the fore in the past few years:

- a fired California teacher as to whom an appellate court upheld a firing based on his posting a gay sex ad on Craig's List.[228]
- multiple fired Pennsylvania health care workers who ostensibly violated HIPAA when posting on Facebook from their own mobile devices;[229]
- a near-record number of Naval commanding officers being fired for sexual harassment, inappropriate relationships, alcohol-related offenses, and other misconduct, attributed in part to social media postings.[230]
- a fired Arizona police officer as to whom the Ninth Circuit upheld the job dismissal based on his "running a website featuring sexually explicit photographs and videos of his wife;"[231]
- a negatively evaluated Pennsylvania high school student-teacher, whose non-receipt of a teaching credential was upheld in light of her posting a photo of herself – captioned the "Drunken Pirate" – on her MySpace page;[232]

---

[227] 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>.

[228] *San Diego U.S.D. v. Comm'n on Prof'l Competence* (Lampedusa), 194 Cal. App. 4th 1454, 124 Cal. Rptr. 3d 320 (Cal. App. 4 Dist. 5/3/11) <www.courtinfo.ca.gov/opinions/documents/D057740.PDF>; Adele Nicholas, *Fired for Using Social Media*, Cal. Lawyer (July 2011) <www.callawyer.com/clstory.cfm?pubdt=NaN&eid=916585&evid=1> ; Bob Egelko, *Teacher's sex ad on Craigs-list grounds for firing*, S.F. Chron. (May 6, 2011) <www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/05/06/BAD61JC06S.DTL&type=printable>.

[229] Virginia Henschel, *Facebook Terminations: Friends Don't Let Friends Talk Smack About Their Job,* LexisNexis Applied Discovery Blog (4/12/10) <http://Facebook-HIPAA-4-12-10.notlong.com>

[230] Chris Whitlock, *Navy Has Spike in Commanding-Officer Firings*, Wash. Post (June 17, 2011) <washingtonpost.com/national/national-security/navy-has-spike-in-commanding-officer-firings-most-for-personal-misconduct/2011/06/14/AGZJj7YH_story.html?hpid=z3>.

[231] *Dible v. City of Chandler*, 515 F.3d 918, 924 (9th Cir. 2008) <ca9.uscourts.gov/datastore/opinions/2008/01/31/0516577.pdf> (discussing *City of San Diego v. Roe*, 543 U.S. 77 (2004) <laws.findlaw.com/us/000/03-1669.html>). *See generally* D. Gregory Valenza, *Overexposed Employees*, Daily J. (Apr. 17, 2009) <shawvalenza.com/publications.php?id=223>.

[232] *Snyder v. Millersville Univ.*, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008) <ecf.paed.uscourts.gov/doc1/15304792325>. *See* Philip Gordon, *First Federal Court Decision to Uphold "Termination" Based on MySpace Content Rejects First Amendment Claim of the "Drunken Pirate,"* Workplace Privacy Counsel (Dec. 8, 2008) <privacyblog.littler.com/2008/12/articles/electronic-resources-policy/first-federal-court-decision-to-uphold-termination-based-on-myspace-content-rejects-first-amendment-claim-of-the-drunken-pirate/print.html>.

- a suspended North Carolina school teacher, who faced possible termination, based on her posting racially derogatory comments on her own Facebook page; [233]
- a Connecticut high school teacher whose contract non-renewal was upheld by a federal district court based on the school superintendent's objections to the teacher's MySpace content and associated communications with students;[234]
- an Iowa community college president, who resigned after a newspaper reported "he was photographed shirtless, while holding a small Coors Light keg over a woman's mouth. The photo, showing [him] with a group of young women and one man, was taken aboard a boat . . ., according to the [newspaper], which received the photo from an area resident;"[235] and
- a police officer whose posts on his MySpace page – about his persona and an ongoing criminal matter -- ostensibly aided the defendant in getting acquitted of a more serious charge at trial.[236]

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.[237] 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

---

[233] Sam Narisi, *Employee uses racial slur in Facebook profile: Can you fire her?* HR Tech News (Feb. 2, 2009) (followed by readers' comments) <http://www.hrtechnews.com/employee-uses-racial-slur-in-facebook-profile-can-you-fire-her/>; Michael P. Stafford, *People, don't you understand: More Teacher Social Networking Woes*, Del. Emp. Law Blog (Nov. 20, 2008) <www.delawareemploymentlawblog.com/2008/11/people_dont_you_understand_mor.html>.

[234] *Spanierman v. Hughes*, 576 F. Supp. 2d 292 (D. Conn. 2008) <https://ecf.ctd.uscourts.gov/doc1/04101870419>. *See generally* Michael P. Stafford, *MySpace and Employment: Another Tale of Woe*, Del. Emp. Law Blog (Oct. 3, 2008) <www.delawareemploymentlawblog.com/2008/10/myspace_and_employment_another.html>.

[235] Sarah Netter, *Keg Folly: College President Resigns Over Photo; President of Iowa Central Community College Gets $400,000 Severance Package*, abcnews (Aug. 29, 2008) <http://abcnews.go.com/US/story?id=5688338&page=1>. *See also* Molly DiBianca, *Off-Duty Conduct of College Pres Leads to Firing*, Del. Emp. Law Blog (Sep. 12, 2008) <http://www.delawareemploymentlawblog.com/2008/09/offduty_conduct_of_college_pre.html>.

[236] Jim Dwyer, *The Officer Who Posted Too Much on MySpace*, N.Y. Times (Mar. 11, 2009) <http://www.nytimes.com/2009/03/11/nyregion/11about.html?pagewanted=print>.

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

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."[238] Generic, vague log-on "banner" warnings as to "monitoring" may be insufficient.[239]

In *TBG Ins. Servs. v. Superior Court (Zieminski)*,[240] the employer had a written policy regarding monitoring of office computer resources as well as work-at-home PC's provided by the company. The employer's policy also forbade use of company-provided PCs for obscene or improper purposes. The employee was terminated for allegedly violating the electronic policies by repeatedly accessing pornographic sites on the Internet while he was at work. The employee claimed that pornographic images were unintentionally "popping up" on his office PC. The employer sought discovery of the employee's home PC. The court held that, under California's constitutional right of privacy, there was no reasonable expectation of privacy when the employee used work-at-home computer for personal matters. The court therefore ordered inspection of the employee's work-at-home computer's hard drive.[241]

Very recently, another state appellate court extended *TBG*-type reasoning to an *employee's own computer* when that machine was physically in a workplace office and connected to the employer's network. *See Sitton v. Print Direction, Inc.*, __ S.E. 2d __2011 WL 4669712 (Ga. App. Sep. 28, 2011) <http://tinyurl.com/Sitton-Print-Ga-App-9-28-11>. 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

---

[238] *See, e.g.*, SAMPLES linked off of Appendix A. For an interesting permutation of the "provided or supported by" concept, *see* MJD, *Brett Favre might want to invest in his own cell phone*, Yahoo Sports (July 23, 2008) <http://sports.yahoo.com/nfl/blog/shutdown_corner/post/Brett-Favre-might-want-to-invest-in-his-own-cell?urn=nfl,95401>.

[239] *See United States v. Long*, 64 M.J. 57 (2006) <armfor.uscourts.gov/opinions/2006Term/05-5002.pdf>. *But see* a case that reached the opposite result based on a factual context in which the banner warning "clearly inform[ed] the employee that he ha[d] no expectation of privacy and state[d] that the computer [wa]s monitored and [could] be intercepted for official use, including criminal prosecution." *United States v. Mosby*, 2008 WL 2961316, at *5 (E.D. Va. July 25, 2008) (distinguishing *Long*; finding "no legitimate, objectively reasonable expectation of privacy . . . work computer" where there was a "detailed warning banner [that the employee] acknowledge[ed] every time he logged onto the computer") <https://ecf.vaed.uscourts.gov/doc1/18901537710>.

[240] *TBG Ins. Servs. Corp. v. Superior Court (Zieminski)*, 96 Cal. App. 4th 443, 117 Cal. Rptr. 2d 155 (2002) http://caselaw.lp.findlaw.com/data2/californiastatecases/b153400.pdf.

[241] Note that, from a computer forensics standpoint, it is entirely possible that the TBG's employee's explanation was valid. Pornographic images may get downloaded to a hard drive even if the computer user does not actually visit any pornographic websites. *See* Brownstone eWorkplace, supra note 2, at 69-70 (.pdf pp. 75-76) <White-Paper-8-09-at-75.notlong.com>. However, if there is evidence – such as web search terms – of the suspect's affirmative conduct, that is another story. *Id.*

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

Id. at *3. Thus, the appellate court affirmed a judgment dismissing all of the employee's common law and state statutory privacy causes of action, the latter of which were brought under OCGA § 16-9-93(a)-(c) <http://www1.legis.ga.gov/legis/2003_04/gacode/16-9-93.html>.

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.[242] Even in a garden-variety wrongful termination case, there may be preservation/spoliation issues. For example, in one case, a former employee was severely sanctioned for discarding her *home* computer at a time when she should have been attempting to land a new job.[243]

The employer's overall right to inspect work-provided computers and portable-media that are physically in the office is typically much more straightforward.[244] Moreover, a physical lock on an employee's office door is typically of no consequence. [245]

b. Inspection/Litigation Provisions

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.[246] Moreover, as soon as

---

[242] *See* Brownstone eWorkplace, supra note 2, at 71 (.pdf p. 77) <http://White-Paper-8-09-at-77.notlong.com>.

[243] *Teague v. Target Corp.*, 2007 U.S. Dist. LEXIS 25368 (W.D.N.C. Apr. 4, 2007) (in case of wrongful termination based on gender, adverse inference against Plaintiff for discarding "home computer . . ., on which she conducted her entire on-line job search after leaving" the employ of Defendant) <http://Teague-Target.notlong.com>. *But see Han v. Futurewei Technologies*, 2011 WL 4344301 (S.D. Cal. 9/15/11) (in wrongful termination case, rejecting ex-employer's/Defendant's request for forensic inspection and copying of exe-employee's/Plaintiff's personal computing devices, because Defendant had provided neither counterclaim allegations nor evidence that Plaintiff had mass-copied/deleted thousands of files in an improper fashion before returning his work-issued laptop) <http://docs.justia.com/cases/federal/district-courts/california/casdce/3:2011cv00831/349569/25/0.pdf?1316160891>.

[244] *See United States v. Durdley*, 2010 U.S. Dist. LEXIS 35422, *19 (N.D. Fla. Mar. 11, 2010) (no Fourth Amendment-protected privacy expectation in contents of a thumb drive "once [employee] attached it to a common-use computer and forgot to remove it") <https://ecf.flnd.uscourts.gov/doc1/04912702108>.

[245] *But see United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007) ("*Ziegler II*") <ca9.uscourts.gov/datastore/opinions/2007/01/29/0530177.pdf>, *rehearing en banc denied by*, 497 F.3d 890 (9th Cir. June 21, 2007) (Order accompanied by various lengthy opinions) <ca9.uscourts.gov/datastore/opinions/2007/06/20/0530177o.pdf> ("*Ziegler III*"), *cert. denied*, 552 U.S. 1105 (2008). *Compare United States v. SDI Future Health Inc.*, 568 F.3d 684, 698 (9th Cir. June 1, 2009) ("except in the case of a small business over which an individual exercises daily management and control, an individual challenging a search of workplace areas beyond his own internal office must generally show some personal connection to the places searched and the materials seized") <ca9.uscourts.gov/datastore/opinions/2009/06/01/07-10261.pdf>.

[246] *See* the *TBG* decision discussed in the preceding sub-section. *See also* the decisions discussed in Brownstone eWorkplace, supra note 2, at 72, at n. 312 (.pdf p. 78) <http://White-Paper-8-09-at-78.notlong.com>.

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.[247] Similarly, where misappropriation of trade secrets is suspected, prompt confiscation of computers, if possible, is a sound proactive approach.

c. International Caveat

Today's increasingly international economy requires American employers to pay close attention to privacy rules in other countries, which may be stringent indeed. Some data rules regulate the entire European Union (EU) region, some are country-specific,[248] 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 limits such rules place on the search-and-discovery of personal data add to the employer considerations addressed throughout Section III of this paper.

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.[249] The United States Department of Commerce has established a "safe harbor" protocol, approved by the EU, to assure compliance with the EU directive. The safe harbor provides for: (1) notice to individuals about the information collected about them; (2) individual choice concerning the disclosure of information; (3) notice and choice principles applied to disclosure to third parties ("onward transfer"); (4) individual access to records for the purpose of correcting inaccurate information; (5) reasonable security steps to protect confidentiality of information; (6) efforts to insure the accuracy of records ("data integrity"); and (7) independent recourse mechanisms to investigate complaints about breaches of privacy.[250]

2. Special Issues Often Ignored: Voicemails/IM's/PDA's

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.[251] Their coverage should include voicemail, IM, PDA's, and other company-issued mobile devices.

---

[247] *Henry v. IAC/Interactive Group*, 2006 U.S. Dist. Lexis 24942 (W.D. Wash. Feb. 14, 2006) (a manager who had threatened to bring discrimination claims took employer-issued laptop with her when told to go on leave, precipitating lengthy motion practice as predicate to employer being able to get back its machine). *See also* forensics decisions cited and linked in Appendix C, at p. C-4.

[248] *See, e.g.*, *Copland v. United Kingdom*, (European Court of Human Rights Apr. 3, 2007) (applying Data Protection Act 1984, which had already replaced by Act of 1998 and which had been enacted pursuant to Article 8 of European Convention on Human Rights) <http://www.thegovernmentsays.com/cache/90069.html>.

[249] *See, e.g.,* Directive 95/46/EC <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Note, however, that, in Finland, the Parliament passed legislation – subsequently signed into law by the Finnish President – with a disparate view; the so-called "Nokia law" apparently gives employers "the right to track workers' e-mails by retaining information about such messages, including the recipients, senders and the time when e-mails have been sent or received." Matti Huuhtanen, *Finnish Parliament approves e-mail tracking law*, The Age (Mar. 5, 2009) <http://news.theage.com.au/action/printArticle?id=405190>. *See also* IOL, *Finland approves email snooping law*, Independent Online (Mar. 14, 2009) <http://www.ioltechnology.co.za/article_print.php?iArticleId=4889373>.

[250] U.S. Dep't of Commerce, *Safe Harbor Overview* ("[t]he United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation[; the EU], however, relies on comprehensive legislation that . . . requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin") <http://www.export.gov/safeharbor/eg_main_018236.asp>.

[251] To learn more, *see* Brownstone, supra note 2, at 74-75 (.pdf pp. 80-81) <http://White-Paper-8-09.notlong.com>.

This issue came to the fore early in 2009 when incoming President Barack Obama ostensibly had to negotiate with his own staffers as to the conditions under which he ultimately got to keep his beloved Blackberry. In addition to laptops, mobile devices such as PDA's can retain sensitive materials that can be easily retrieved by hackers if data is not properly "hard-wiped" before disposal of the device.

3. Prohibitions/Restrictions on Blogging, Posting, Social-Networking, Twittering and the Like[252]

Determining an organization's official position on employee web postings is a much harder task than it appears at first glance.[253] 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 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:

- *Blog Content Impact on Entity's Image*: For instance, even if the content does not give rise to legal liability (either to the employer or the employee), it may cast the organization in an unfavorable light. And, readers may come across the content without intentionally accessing it. For example, the content of may appear in results generated by search engines. With more and more companies doing independent research on their customers, vendors and business partners, an employee's postings may have the unintended effect of driving away customers before a company ever knows about the potential business opportunity. Notwithstanding the risk, many organizations also feel blogs present a new forum for communicating what is good about the entity and its products and/or services.
- *Corporate Image and Culture*: More importantly, a private company must consider its image and corporate culture before finalizing an official position on employee blogging. High-technology companies, who wish to convey their technological savvy and that of their employees, may decide that their image requires a pro-UGC policy. Companies who pride themselves on employee-friendliness and open communication may decide that they should also encourage blogging to further their corporate culture.
- *UGC as Part of eDiscovery*: UGC may also make an appearance during litigation. Such web content has add already added another layer of complexity to the eDiscovery landscape, potentially requiring employers to search for and produce additional information.

A 2009 public sector example of risk/benefit assessment involved the Information Technology (IT) powers-that-be at the Maryland legislature. The IT leaders wrestled with – and flip-flopped as to – whether it

---

[252] To learn more, *see* Brownstone, supra note 2, at 75-79 (.pdf pp. 81-85) <http://White-Paper-8-09.notlong.com>.

[253] *See generally* Amy Komoroski Wiwi and Lawren Briscoe, *How Employers can Balance Social Media Rights and Obligations*, N. J. L. J. (May 10, 2011) <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202493353027>.

is appropriate for elected legislators to be interacting with constituents via social-networking sites.[254] In the Maryland situation and in other more recent scenarios, one concern entails the dangers of malware that can spread via: legitimate Facebook-type sites; and/or via "spoofing" links in e-mail messages that are designed to fool employees who regularly receive legitimate Facebook messages in their work e-mail accounts.[255] Another risk is that the employer's own Web 2.0 account might get hijacked.[256] However, because many constituents are heavy users of social media, politicians often incorporate social media into their campaigns and professional activities.[257]

In the last few years, though, elected official's use of Twitter and the like have, of course, become *de rigeur*. *See, e.g.,* Tim Mak, *Survey: Congress uses Twitter more than millennials*, Politico (Sep. 29, 2011) (citing AP) <politico.com/news/stories/0911/64689.html>; Fearless, *The U.S. Congressional Twitter Directory* (July 28, 2011) <http://fearlessrevolution.com/blog/the-us-congressional-twitter-directory.html>; beSpacific, *GovTwit - the Government Social Media Directory* (purporting to host "the world's largest list of government agencies and elected officials on Twitter") <http://govtwit.com/>.

When the employees in question are not politicians, though, what do you think the employer should do on this front? In any event, at the end of the day, settling on a philosophy requires an organization company to do a self assessment and determine what balance between technological savvy, forthright communication, and legal risk best fits with the corporate culture and image the company wishes to maintain.[258]

In that vein, the federal Veterans Administration has published a Social Media Policy that "*Establishes Responsible Use for Web-based Collaboration Tools*." *VA Publishes Social Media Policy* (Aug. 16, 2011) <www.va.gov/opa/pressrel/pressrelease.cfm?id=2150>. Among the issues in the new VA policy

---

[254] Helderman, Rosalind S., *Legislators Log Back On To Facebook*, Wash. Post (Feb. 11, 2009) <washingtonpost.com/wp-dyn/content/article/2009/02/10/AR2009021003301_pf.html>; Helderman, Rosalind S., *Plug Pulled on Md. Legislature's Facebook, MySpace for Fear of Viruses*, Wash. Post (Feb. 7, 2009) <washingtonpost.com/wp-dyn/content/article/2009/02/06/AR2009020602922.html>. *See also 'Koobface' worm resurfaces on Facebook, MySpace*, Wash. Post (Mar. 3, 2009); Kopytoff, Verne, *Koobface computer virus attacks Facebook users*, S.F. Chronicle (Dec. 6, 2008) <sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/12/06/BU0R14IR63.DTL&type=printable>; Robert Vamosi, *Facebook worm feeds off Google's reputation*, CNET (Oct. 29, 2008) <news.cnet.com/8301-1009_3-10078353-83.html>.

[255] Emily Steel and Geoffrey A. Fowler, *Facebook in Privacy Breach; Top-Ranked Applications Transmit Personal IDs*, Wall St. J. (Oct. 18, 2010) <online.wsj.com/article/SB10001424052702304772804575558484075236968.html#printMode>; Brad Stone, *Viruses That Leave Victims Red in the Facebook*, N.Y. Times (Dec 14, 2009) <nytimes.com/2009/12/14/technology/internet/14virus.html?pagewanted=print>; Cisco, *2009 Annual Security Report*; *Highlighting global security threats and trends* (Dec. 4, 2009) <cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf>.

[256] *See, e.g., New password-stealing virus targets Facebook,* Reuters (Mar. 17, 2010) <reuters.com/assets/print?aid=USTRE62G5A420100318> BJ Lutz, *United Airlines Caught in Twitter Hack; High-profile accounts worldwide compromised overnight*, NBC Chicago (Feb. 26, 2010) <http://tinyurl.com/Lutz-UAL-2-26-10>.

[257] *See Twitter Town Hall Showcases Social Media's Political Potential*, PBS NewsHour (July 6, 2011) <http://www.pbs.org/newshour/bb/politics/july-dec11/twitter_07-06.html>; Tom Cheredar, *Obama's Twitter Account: Now with 100 Percent More President*, Social Beat (June 18, 2011) <http://venturebeat.com/2011/06/18/obama-tweets/>. But politicians' social media use is not always a success: see, e.g., *Meg Whitman's campaign shows how not to use Twitter*, InfoWorld (Oct. 20, 2010) <http://www.infoworld.com/print/141335> (gubernatorial candidate's staff tweeted a link to a video of a guitar-playing man in a tutu instead of to an endorsement by a group of sheriffs).

[258] *See generally* Nancy Dupre Barnes, Ph.D., and Frederick R. Barnes, J.D., *Equipping Your Organization for the Social Networking Game*, ARMA Info. Mgmt. (Nov./Dec. 2009) <content.arma.org/IMM/NovDec2009/IMM1109equippingyourorganizationforthesocial.aspx; Philip M. Berkowitz, *Social Networking and the New Workplace*, N.Y.L.J. (Nov. 12, 2009) <law.com/jsp/article.jsp?id=1202435367912>; Symantec, *Employee Web Use and Misuse: Companies, their employees and the Internet* (Oct. 22, 2009) <http://downloads.messagelabs.com/dotcom/Employee_Web_Use+Misuse_v04.pdf>.

<va.gov/vapubs/viewPublication.asp?Pub_ID=551&FType=2> are information-security threats of the sort that concerned the Maryland Legislature's IT leader back in 2009.

The *Pietrylo* decision discussed above highlights the challenges employers face with respect to employees' blogs and social networking sites that contain work-related speech.[259] While the decision did not restrict an employer's right to monitor communications and information within its own computer networks, it demonstrates the risks of attempting to access an employee's restricted online content without the employee's authorization.[260] Yet, when implementing written policies that address employee 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.[261] 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.[262]

The NLRB has increasingly targeted employers' social media restrictions. In April 2011, the NLRB's Acting General Counsel Lafe E. Solomon adopted the position that employees' social media activities can trigger federal labor law rights even for non-union employees,[263] and he added social media to the list of subjects in which he was taking particular interest.[264] Then, in August 2011, Solomon released a report concerning the outcomes of investigations into 14 respective NLRB social media cases from the preceding year. 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 the report itself, *Report of the Acting General Counsel Concerning Social Media Cases, Memorandum*, OM 11-74 (Aug. 18, 2011) <http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e743>. *See also* John McLachlan, *Not As Bad As We*

---

[259] *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.

[260] *Id. See also Konop v. Hawaiian Airlines (Stored Communications Act* applies to posts on a restricted social media page); *Theofel v. Fary-Jones,* (use of false pretences to gain access to such sites would constitute unauthorized access in violation of the SCA), both discussed in footnotes 64-65 and accompanying text in Section II(B)(1)(a) above.

[261] *Id.*

[262] 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) <http://www.docstoc.com/docs/50764618/Sears-Holdings-%28Roebucks%29-18-CA-19081-120409>. The NLRB's press release announcing the *AMR* settlement agreement may provide guidance to employers drafting social media policies: "Under 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." *NLRB Settlement Agreement in the Matter of AMR of Connecticut, Inc.* (Feb. 7, 2011) <http://www.minnesotaemploymentlawreport.com/NLRB%20Facebook%20Settlement.pdf>. *See also* Walter Stella & Jessica Boar, *Social Media Policy After NLRB, Facebook Settlement*, The Recorder (Mar. 23, 2011) <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202487457090>.

[263] 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>.

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

Feared: NLRB Issues Guidance On Social Media, Fisher & Phillips LLP Labor Letter (Sep. 2011) <http://www.laborlawyers.com/showarticle.aspx?Show=14355&Type=1119&cat=3386&PrintPage=True>.

Most recently, in January 2012, Acting GC Solomon issued another report, covering 14 cases, 7 of which involved social media: NLRB Office of Public Affairs, *Acting General Counsel issues second social media report*, News Release (Jan. 25, 2012) <http://www.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/09031d458056e743>.

Social-media posts can be protected concerted activity under the NLRA.[265] For example, firing an employee because of a Facebook post that criticized the hot dogs and bottled water served to customers at a sales event would run afoul of the NLRA protection for concerted activity. *Karl Knauz Motors*, 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>. Moreover, 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 that NLRA protection.[266] *See Hispanics United of Buffalo, Inc.*, Case No. 3-CA-27872 (Buffalo, NY Sep. 2, 2011) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580622877>. In *Hispanics United*, the ALJ held that a New York nonprofit unlawfully terminated five employees for posting criticisms of a co-worker on Facebook. In response to a comment from a coworker, one of the five employees posted on her Facebook page on Saturday (a non-work day) that "a coworker feels that we don't help our clients enough . . . My fellow coworkers how do u feel?" (The original poster was apparently trying to get the other posters terminated or at least disciplined.) The post elicited a number of responses from the four other employees about their difficult working conditions. After the coworker who made the original comment complained about the posts, the Executive Director of the nonprofit immediately terminated the five employees and informed them that the posts constituted bullying and harassment.

The NLRB issued a complaint against the employer, asserting that the terminations violated Section 8(a)(1) of the NLRA, which provides that it is unlawful to "interfere with, restrain or coerce" employees in the exercise of their Section 7 rights. Among other things, Section 7 protects the rights of all employees (union and non-union) to engage in "concerted activities" for the purpose of "mutual aid or protection." In *Hispanics*, the ALJ eventually determined that the Facebook postings, in reaction to a coworker's criticisms of the manner in which the employees did their jobs, constituted protected activity. The judge held that it was irrelevant that the employees "were not trying to change their working conditions and that they did not communicate their concerns" to their employer, because the employees "were taking a first step towards group action to defend themselves against the accusations they could reasonably believe [the coworker] was going to make to management." The ALJ ordered the employer to reinstate the employees and make them whole for lost earnings and benefits.

But when posts do not relate to the terms and conditions of employment, the NLRB has found no violation.[267] For example in *Knauz* -- in the same decision in which the Administrative Law Judge (ALJ) ultimately found that the above sales event criticism was protected, the ALJ upheld an employee's dismissal

---

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

[266] *Hispanics United of Buffalo, Inc.*, Complaint (May 17, 2011) <www.employmentlawmatters.net/uploads/file/5-17-11-Facebook%20firing-Hispanics%20United.pdf>. *See also NLRB Focused On Employee Social Media* Post, Fenwick Employment Brief (Sep. 19, 2011) <fenwick.com/publications/6.5.4.asp?mid=76&WT.mc_id=EB_091911#nlrb>, on which the ensuing *Hispanics United* discussion is largely based.

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

based on a different kind of posting.[268] *Id.* There, the employer had terminated a Chicago-area BMW employee for his Facebook post in which he commented on two work-related events. First, the employee mocked the "Ultimate Driving Event" – at which the dealership served hot dogs and water – as cheap and conveying the wrong message to potential customers. The post followed discussion with, and voiced the concerns of, co-workers whose salaries were based on commissions and who had access to and commented on the post. Second, the employee posted photos of an accident caused by a 13-year-old driving an LR4 into a pond at an adjacent (employer-owned) car dealership and commented: "This is your car: This is your car on drugs."

The *Knauz* ALJ ruled that the commentary on the Ultimate Driving Event was protected activity, but concluded the termination resulted from the posting of the accident photos and, therefore, was not wrongful. In recognizing no protection for the accident-related post, the judge observed it was done "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." *Id.* Also of interest, the ALJ concluded that several provisions in the employer's handbook – seemingly innocuous prohibitions on language injurious to the employer's image or reputation, unauthorized interviews, and communications with non-employees regarding personnel matters – violated the NLRA because they were overbroad with the potential to chill lawful, employee concerted action. *Id.*

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 (TAW, Inc.), an employee complained to her employer that a company accounting practice could constitute fraud, and then posted her belief on her Facebook page. *See TAW, Inc.*, Case 26-CA-063082, GC Advice Memo (Nov. 22, 2011) <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580755f55>. The employer met with the employee and external auditors, who assured her that the employer was not engaged in fraud. A few days after the meeting, the employer asked her to remove the post. She refused and was terminated. The post did not constitute protected activity because when she was asked to remove the post, she knew that the employer was not engaged in fraud. Thus, the post was false and her refusal to remove it was not protected under the NLRA. *Id. See also* Fenwick & West, *NLRB General Counsel Issues Pro-Employer Social Media Decisions*, Fenwick Employment Brief (Jan. 10, 2012) <fenwick.com/publications/6.5.4.asp?mid=80#general>, from which this summary was adapted.

The NLRB has signaled that it will be similarly concerned with employers' actions based on employees' Twitter activities. On May 2, 2011, Thomson Reuters and the Newspaper Guild settled a labor dispute, heading off an NLRB complaint that would have been the first NLRB action based on a Twitter post. The NLRB had planned to file a complaint against Thomson Reuters, accusing the company of illegally reprimanding a reporter for her public tweet criticizing management. Employees had been invited to post thoughts on what would make the company the best place to work. The employee in question, who was also the Newspaper Guild's representative, tweeted, "One way to make this the best place to work is to deal honestly with Guild members." Then, her supervisor called to remind her of the company's policy prohibiting employees from posting content that would damage the company's reputation. The NLRB viewed the phone call as potentially chilling the employee's exercise of her NLRA rights.[269]

---

[268] *See Employer Defeats Challenge to Termination Over Facebook Post*, Fenwick Employment Brief (Oct. 11, 2011) <http://www.fenwick.com/publications/6.5.4.asp?mid=77&WT.mc_id=EB_101111#nb>, on which the ensuing *Knauz* discussion is largely based.

[269] *See* Steven Greenhouse, *Labor Panel to Press Reuters Over Reaction to Post*, The New York Times (Apr. 6, 2011) <http://www.nytimes.com/2011/04/07/business/media/07twitter.html>.

The NLRB's vigorous activity in the Web 2.0 arena may be a harbinger of similar unfair labor practice complaints brought by public sector employees. The settlements and proceedings to date are non-conclusive as to where the pertinent boundaries may ultimately be drawn.

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,[270] 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.

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.[271] Note, though, that, in 2007, a federal court decision ostensibly gave a state government very broad authority to regulate the blogs which its employees visit – as long as there is no viewpoint-based discrimination.[272] The law in this area is still relatively nascent. Thus, one 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.[273]

---

[270] For a detailed discussion of an outlier decision that expanded the scope of third-party liability under New Jersey law, *Doe v. XYC Corp.*, 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005) <http://lawlibrary.rutgers.edu/decisions/appellate/a2909-04.opn.html>, *see* Brownstone eWorkplace, supra note 2, at 80-81 (.pdf pp. 86-87) <http://White-Paper-8-09-at-86.notlong.com>. *But compare Maypark v. Securitas Sec. Servs. USA, Inc.,* 775 N.W.2d 270, 276 (Wis. Ct. App. Sep. 1, 2009) (rejecting negligent training/supervision claim because "employers have no duty to supervise employees' private conduct or to persistently scan the world wide web to ferret out potential employee misconduct") <http://Maypark-Wisc-App-9-1-09.notlong.com>. For a more recent public sector scenario, *see* Complaint, *Guardian Civic League v. Philadelphia Police Dep't* (E.D. Pa. 7/15/09) linked from <http://Philly-Sgt-7-15-09.notlong.com>; *see also* eDocket, available at <https://ecf.paed.uscourts.gov/cgi-bin/DktRpt.pl?675836827147751-L_942_0-1>.

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

[272] *Nickolas v. Fletcher*, 2007 U.S. Dist. LEXIS 23843 (E.D. Ky. March 30, 2007 (denying preliminary injunction against state's policy of prohibiting state employees from accessing blogs; finding state's policy was reasonable, was not view-point based discrimination and was unlikely to violate First Amendment) <https://ecf.kyed.uscourts.gov/cgi-bin/show_case_doc?30,50167,,,,,136,1>, *stay granted pending appeal*, 2007 U.S. Dist. LEXIS 58351 (E.D. Ky. Aug. 9, 2007) <https://ecf.kyed.uscourts.gov/doc1/0811546896>. As noted in Section II(B)(4) above, the NLRB reached an analogous result in the different context of employee e-mails that do address a particular type of content, namely union activity. *The Guard Publishing Company, d/b/a The Register-Guard*, Cases 36-CA-8743-1, et al.

[273] *See, e.g.*, these segments of the Samples found in Appendix D of <http://White-Paper-8-09.notlong.com>: SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 1, §§ I(D)(4), at App. D-2, IV(A), at App. D-4; SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 2, § V, at App. D-8; SAMPLE ELECTRONIC MAIL POLICY, § II, at App. D-10; *see also Dep't Of Education v. Choudhri*, OATH Index No. 722/06 (N.Y.C. Office Of Admin. T & H 3/9/06) <http://files.findlaw.com/news.findlaw.com/hdocs/docs/nyc/doechoudri30906opn.pdf>. *Compare Lee v. PMSI, Inc.*, 2011 WL 1742028 (M.D. Fla. 5/6/11) (dismissing employer's CFAA counterclaim, which was based on allegations that ex-employee had engaged in " 'excessive internet usage' and 'visit[ed] personal websites such as Facebook and monitor[ed] and [sent] personal email through her Verizon web mail account.' ") (alterations in original) <http://www.noncompetenews.com/file.axd?file=2011/5/Lee%20v.%20PMSI.pdf>.

D. Periodic Training

Some identify the fundamental principles of policy implementation as "The Three E's," namely Establish, Educate and Enforce.[274] Anyway, having developed written policies, employers should provide periodic training on the contents of such policies. The training should have a rules-of-law underpinning, an Information Technology (IT) component and be offered not only at the time of roll-out of a new regime but also periodically. Consequently, veteran employees can receive refresher training; and new employees can be educated as part of, or a follow-up to, their orientation. Some key subject areas should include e-mail "netiquette" as well as privilege/confidentiality. Workers should learn to be circumspect about what they put in writing, especially in e-mail. The "writing for multiple audiences" concept addresses the capacity for e-mail to proliferate and end up all over the world. The author's firm cautions clients' employees via a proprietary "Green Eggs and Ham" mantra.[275] Examples of inappropriate content include sexual imagery, defamatory language, "name-calling" and discussion of predatory/anti-competitive acts. Many lists of "no-no's" are on the web.[276] In addition, a lawyer should train employees on best practices regarding written communications with attorneys. Some considerations in this arena: providing an e-mail message – and, if any, the accompanying attachment(s) – to counsel *before* circulating them to others (*i.e.*, instead of counsel receiving the item as a "cc" as it gets sent to others); refraining from re-stating counsel's legal advice; and avoiding excessive forwardings, re-distributions and "Reply to All". Note that there are ways to implement the triggering of an automated warning prompt each time an employee clicks on "Reply to All".

E. Information-Security Compliance Considerations

Data leakages can occur in many different ways, including hacking of networks, loss or theft of mobile devices, improper disposal enabling dumpster-diving, human error, employees' internet activity and phishing schemes. Yet, IT processes tend to be insufficiently controlled. Employers of all sorts can improve their information-security practices by focusing on the "CIA" (Confidentiality, Integrity and Availability) of electronic data. Three major frameworks provide guidance for electronic information management. As to security breaches, particular best practices are required for federal agencies and warranted for others. To succeed, though, technological change cannot occur in a vacuum. Computer technology must be but one part of a three-pronged approach that covers: administration (philosophy, policies, etc.); education (of executives, managers and employees); and technology (hardware, software and other "solutions" to implement compliance frameworks and other best practices). As a key IT-related example, employees – especially those dealing with hyper-confidential content, in Legal Departments and/or negotiating contracts via multiple rounds of e-mail exchanges – should learn of the potential of dangers of disseminating Microsoft Office e-mail attachments to people outside your company without first scrubbing the metadata. Microsoft's own menus and tools entail many steps and are not sufficiently thorough. Two affordable, user-friendly tools are Payne Consulting Group's Metadata Assistant and Workshare's Protect.

---

[274] 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>.

[275] Brownstone eWorkplace, supra note, 2 at 4 n.15, (.pdf p. 10 n. 15) <http://White-Paper-8-09-at-10.notlong.com.>; *id.* at 82-83 (.pdf pp. 88-89); Meridith Levinson, *10 Things You Should Never Write in an E-Mail or IM*, CIO (Dec. 1, 2008) <http://blogs.cio.com/print/6932>.

[276] *See, e.g.,* Andrew G. Rosen, *18 Common Work E-mail Mistakes* (Jan. 18, 2011) <money.usnews.com/money/blogs/outside-voices-careers/2011/01/18/18-common-work-e-mail-mistakes_print.html> ; Jenna Goudreau, *What Not To Say At Work*, Forbes (Nov. 8, 2010) (linking to top "10" slides/photos) <forbes.com/2010/11/08/what-not-to-say-at-work-career-forbes-woman-leadership-coworkers_slide.html>; Kerry A. Dolan, Worst Facebook Posting Gaffes, Forbes (Nov. 5, 2010) (linking to top 11 slides/photos) <forbes.com/2010/11/05/safety-security-privacy-technology-facebook-posts.html>. *See also* Top 5 Sick Day FAILs: Pics, Videos, Links, News, BuzzFeed (last visited Oct. 22, 2011) <http://www.buzzfeed.com/sneeze/top-5-sick-day-fails-u2j>; *Call centre worker caught out by boss after posting 'sickie' plan on 'Facebook'*, Daily Mail (Oct. 23, 2008) <http://www.dailymail.co.uk/news/article-1080010/Call-centre-worker-caught-boss-posting-sickie-plan-Facebook.html>.

APPENDIX A

Robert D. Brownstone – Materials & Resources –

SAMPLE TECHNOLOGY-ACCEPTABLE-USE POLICIES ("TAUP's") – @ 2/16/12

- ***Generic TAUP's – Samples appended to 8/28/09 NELI White Paper***:
  - **Pages D-1 through D-17 (.pdf pp. 142-58) (blogging policy should be expanded to cover all Web 2.0 sites/pages, incl. employer-sponsored and personal)**

    <http://fenwick.com/docstore/publications/EIM/eWorkplace_Policies_Materials_Public_Sector_EEO_8-28-09.pdf#page=142>

- ***Web-2.0/Social-Media Policies – Non-Fenwick-Drafted Generic Samples:***
  - 195 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")
  - <http://www.ibm.com/blogs/zz/en/guidelines.html> ("IBM Social Computing Guidelines ")
  - <http://domino.research.ibm.com/comm/research_projects.nsf/pages/virtualworlds.IBMVirtualWorldGuidelines.html> ("IBM Virtual World Guidelines")
  - <va.gov/vapubs/viewPublication.asp?Pub_ID=551&FType=2> (new VA Policy)
  - 178 Reports at <http://socialmediagovernance.com/studies/>
  - <www.records.ncdcr.gov/guides/best_practices_socialmedia_usage_20091217.pdf>
  - <www.utahta.wikispaces.net/file/view/State+of+Utah+Social+Media+Guidelines+9.29.pdf>
  - <http://www.law.com/jsp/tal/PubArticleTAL.jsp?id=1202426674355>, linking to sample:
    - <http://shorl.com/mogustemymidru> (Jaffe PR Sample)
  - <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)

- ***Related Helpful Resources***
  - <http://www.records.ncdcr.gov/>
  - <http://www.bicklaw.com/Publications/LAWFULMININGOFSOCIALNETWORKS.htm>
  - <http://www.delawareemploymentlawblog.com/privacy-in-the-workplace/>
  - <http://www.delawareemploymentlawblog.com/social-media-in-the-workplace/>
  - <http://mashable.com/2009/04/28/facebook-privacy-settings>

Appendix B – Social-Media eDiscovery – Brownstone Bibliography (2/16/12)

SOME Social-Media eDiscovery Decisions

- *Largent v. Reed*, No. 2009-1823 **(Pa. Ct. Common Pleas Franklin Cty. 11/8/11)** <http://druganddevicelaw.net/Opinions%20in%20blog/Largent.pdf>
- *Romano v. Steelcase*, 907 N.Y.S. 2d 650, at *5 **(N.Y. Sup. 9/21/10)** <courts.state.ny.us/Reporter/3dseries/2010/2010_20388.htm>
- *McMillen v. Hummingbird Speedway, Inc*., No. 113-2010 CD **(Pa. C.P. Jefferson Cty. 9/9/10)** <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. 6/3/10)** <https://ecf.tnmd.uscourts.gov/doc1/16911303989>
- *Crispin v. Christian Audigier, Inc.*, No. CV 09-09509 MMM (JEMx) **(C.D. Cal. 5/26/10)** <ecf.cacd.uscourts.gov/doc1/031110245153>
- *E.E.O.C. v. Simply Storage Management, LLC*, 270 F.R.D. 430, 434 **(S.D. Ind. 5/11/10)** (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>
- *U.S. v. Phaknikone*, 605 F.3d 1099, 1107 **(11th Cir. 5/10/10)** <ca11.uscourts.gov/opinions/ops/200910084.pdf>
- *Nguyen v. Starbucks Coffee Corp.*, 2009 WL 4730899 **(N.D. Cal. 12/7/09)** <https://ecf.cand.uscourts.gov/doc1/03516287723>
- *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, 2007 U.S. Dist. LEXIS 2379 **(D. Nev. 1/9/07)** <https://ecf.nvd.uscourts.gov/doc1/11511167020>

eDiscovery-Law Online Libraries

- Applied Discovery, *Law Library* <http://www.applieddiscovery.com/ws_display.asp?filter=Online%20Law%20Library>
    - *Case Summaries* <http://www.applieddiscovery.com/ws_display.asp?filter=Case%20Summaries>
    - *By Topic* <http://www.applieddiscovery.com/ws_display.asp?filter=View%20By%20Topic>
    - *By Jurisdiction* <http://www.applieddiscovery.com/ws_display.asp?filter=View%20By%20Jurisdiction>
- K&L, Gates *Blog, etc.* <http://www.ediscoverylaw.com/>
    - *Case Database* <https://extranet1.klgates.com/ediscovery/>
- Kroll, OnTrack Data, *Resource Library* <http://www.krollontrack.com/resource-library/>
    - *Database* (searchable by topic and/or jurisdiction) <http://www.krollontrack.com/resource-library/case-law/>
        - *Static List -- by Topic* <http://www.krollontrack.com/library/topic.pdf>
        - *Static List -- by Jurisdiction* <http://www.krollontrack.com/library/jurisdiction.pdf>

eDiscovery-Law Blogs

- *Bow Tie Law's Blog* <http://bowtielaw.wordpress.com>
- *eDiscovery Insights* <http://www.ediscoverycalifornia.com>
- *eDiscovery Team* Blog <http://e-discoveryteam.com/>
- *Electronic Discovery Navigator* <http://www.ediscoverynavigator.com/>

Appendix B – Social-Media eDiscovery – Brownstone Bibliography (2/16/12)

Metadata Bibliography by Robert Brownstone

- <fenwick.com/docstore/publications/EIM/Metadata_Brownstone_Bibliography_6-3-11.pdf>

Computer Technology Terminology Online Glossaries

- How Stuff Works <http://computer.howstuffworks.com/>
- 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 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>
- <http://viaforensics.com/education/computer-forensics-ediscovery-glossary/>

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) <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) <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) <http://www.fenwick.com/docstore/publications/Litigation/ediscovery.pdf>

Shorter eDiscovery/ESI Articles by Robert Brownstone

- *See* full Brownstone Bibliogrpahy at <http://www.fenwick.com/attorneys/4.2.1.asp?aid=544>

eDiscovery Slide Decks *(SOME)* by Robert Brownstone

(ONLY SOME of the ones available online)

- *See* full Brownstone Bibliography at <http://www.fenwick.com/attorneys/4.2.1.asp?aid=544>

eDiscovery Articles Featuring and/or Quoting Robert Brownstone:

- *See* full Brownstone Bibliography at <http://www.fenwick.com/attorneys/4.2.1.asp?aid=544>

APPENDIX C – Brownstone – Resources re: Attorney-Client Privilege, etc. (2/16/12)

I. Attorney-Client Privilege Opinions

- *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://docs.justia.com/cases/federal/district-courts/washington/wawdce/2:2010cv01022/168521/108/0.pdf?1320941987>

- *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* <americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_11_459.authcheckdam.pdf>

    - *Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel* <americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_11_460.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>

- *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) <courtinfo.ca.gov/opinions/archive/C059133.PDF>

- *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") <ecf.ilnd.uscourts.gov/doc1/06718389059> or <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/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") <lawlibrary.rutgers.edu/decisions/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 employer Computer Usage Policy's express warnings that employees should use their computers solely for "business purposes" and that they "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>

- *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>

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

- *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) <courts.state.me.us/court_info/opinions/2009%20documents/09me71fi.pdf>

- *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**) (distinguishing *Jiang*, in employment breach of contract action; Plaintiff's communications with attorney regarding litigation, transmitted over Defendant's email system, not protected by privilege or work-product, in light of "no personal use" e-mail policy combined with stated policy allowing for employer monitoring) <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") <jenner.com/files/tbl_s69NewsDocumentOrder/FileUpload500/3492/Sims%20v.%20Lakeside%20School.pdf>

- *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 is clear and unambiguous[; P]laintiffs disregarded the admonishment voluntarily and, as a consequence, have stripped from the e-mail messages . . . the confidential cloak") <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://www.gesmer.com/upload/download.php?id_files=65>

- *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>

- *Asia Global Crossing, Ltd., In re*, 322 B.R. 247, 251, 259 (**Bankr. S.D.N.Y. 3/21/05**) ("[a]ssuming a communication is otherwise privileged, the use of the company's e-mail system does not, without more, destroy the privilege; however, no waiver of attorney-client privilege because "evidence [wa]s equivocal regarding the existence or notice of corporate policies") <http://www.internetlibrary.com/pdf/In-re-Asia-Global-Crossing-SD-NY-Bankruptcy.pdf>

- ***Compare*** *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 of sexual harassment and 'nventory questions' 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>)

APPENDIX C – Brownstone – Resources re: Attorney-Client Privilege, etc. (2/16/12)

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 (Mar. 2011) <fenwick.com/docstore/Publications/EIM/fenwick_west_brownstone_ghassemi-vanni_cho_article.pdf>
- Daniel J. McGravey and Amy C. Lachowicz, *Can Employers Review Electronic Messages?* Pa. Legal Intelligencer (Sep. 14, 2010) <law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202471935042>
- 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>
- Jeffrey Campolongo, *ABA Opinions Clarify Ethical Obligations in E-Mail Interception*, Pa. Legal Intelligencer (9/26/11) <www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202516689146>
- September 26, 2011 Allison Shields, *Attorney-Client Confidentiality and Email*, Lawyerist (9/21/11) <http://lawyerist.com/attorney-client-confidentiality-email/>
- Robert D. Brownstone, *Metadata & Electronic Redaction -- Partial Bibliography* (6/3/11) <www.fenwick.com/docstore/publications/EIM/Metadata_Brownstone_Bibliography_6-3-11.pdf>
- Joshua Davis, *Some Employee E-mails May Be Privileged*, Recorder (6/18/10) <http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202462837364>
- 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/>
- Michael Booth, *Privilege Trumps Company E-Mail Surveillance*, N.J.L.J. (4/1/10) <http://www.law.com/jsp/nj/PubArticleNJ.jsp?id=1202447264728>
- 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/cc/PubArticleCC.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>

III. Additional Privacy Decisions in Other Contexts re: Laptop or Desktop Contents:

- ***Various decisions compiled at these footnotes & accompanying text***
  - Robert D. Brownstone, *Workplace Privacy Policies*, Nat'l Emp. L. Inst. (NELI) (Aug. 2009) <fenwick.com/docstore/publications/EIM/eWorkplace_Policies_Materials_Public_Sector_EEO_8-28-09.pdf > (more recent, shorter version available from author on request):
    - footnote 60 @ .pdf p. 20 (White Paper p. 14); footnotes 305-09 @ .pdf pp. 75-77 (White Paper pp. 69-71); and footnote 325 @ .pdf p. 79 (White Paper p. 73)
- ***Various decisions compiled at these pages***
  - Robert D. 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):
    - 2006 L. Rev. article, at pp. 32-33 <http://www.ncjolt.org/sites/default/files/8_nc_jl_tech_1.pdf#page=32>
    - 2007 Supp., at p. 8 <fenwick.com/docstore/publications/EIM/NC_JOLT_eDiscovery_Supplement.pdf#page=8>
- ***Overbreadth of discovery via forensics***
  - *Han v. Futurewei Technologies*, 2011 WL 4344301 (**S.D. Cal. 9/15/11**) (in wrongful termination case, rejecting ex-employer's/Defendant's request for forensic inspection and copying of exe-employee's/Plaintiff's personal computing devices, because Defendant had provided neither counterclaim allegations nor evidence that Plaintiff had mass-copied/deleted thousands of files in an improper fashion before returning his work-issued laptop) <http://docs.justia.com/cases/federal/district-courts/california/casdce/3:2011cv00831/349569/25/0.pdf?1316160891>
  - *Bennett v. Martin*, 2009-**Ohio**-6195, 2009 WL 4048111(**10th App. Dist. 11/24/09**) <http://www.supremecourt.ohio.gov/rod/docs/pdf/10/2009/2009-ohio-6195.pdf>
  - *Cornwall v. Northern Ohio Surgical Ctr*., Ltd., 2009-**Ohio**-6975, 2009 WL 5174172 (**6th App. Dist. 12/31/09**) <www.supremecourt.ohio.gov/rod/docs/pdf/6/2009/2009-ohio-6975.pdf>
  - *In re Weekley Homes L.P.*, 295 S.W. 3d 309 (**Tex. 8/28/09**) (conclusory assertions as to hoped-for circumstantial evidence insufficient to warrant capture of four hard disc images) <http://www.supreme.courts.state.tx.us/historical/2009/aug/080836.pdf>
  - *John B. v. Goetz*, 2008 WL 2520487, 2008 U.S. App. LEXIS 13459 (**6th Cir. 6/26/08**) (vacating district court order that had required forensic captures of ≥ 50 computers' hard drives, based in part on privacy/confidentiality concerns) <www.ca6.uscourts.gov/opinions.pdf/08a0226p-06.pdf>

Full Brownstone Bibliography at <fenwick.com/attorneys/4.2.1.asp?aid=544>

Appendix D – Robert D. Brownstone – Partial Bibliography – CFAA Decisions on Viability of Employer Claim vs. (Ex)-Employee (2/16/12)

Articles *(reverse chron order)*

- Fenwick & West LLP, *Ninth Circuit Holds Computer Fraud and Abuse Act Criminalizes Employee's Access To Information In Violation Of Employer's Express Access Limitations, Lit. Alert* (May 2, 2011) <fenwick.com/docstore/Publications/Litigation/Litigation_Alert_05-02-11.pdf>
- 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) <http://www.fenwick.com/publications/6.5.4.asp?mid=51&WT.mc_id=EB_101509#employee>
- Rubel, Ilana S. (also of Fenwick & West), *Screen Grabs*, Daily J. (3/13/09), available at <http://www.fenwick.com/docstore/Publications/Litigation/Shrinking_Prospects_CFAA.pdf>
- Morphy, Erika, *The Computer Fraud Act: Bending a Law to Fit a Notorious Case*, E-Commerce Times (12/09/08) (quoting Robert D. Brownstone) <http://www.ecommercetimes.com/story/65424.html#>

U.S. Circuit Court Decisions *(alphabetical order)*

- *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. Mar. 8, 2006), <http://caselaw.findlaw.com/us-7th-circuit/1392048.html>, *on subsequent appeal*, 445 F.3d 749 (7th Cir. July 25, 2006) <http://caselaw.findlaw.com/us-7th-circuit/1115559.html>
- *John*, *U.S. v.,* 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>
- *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133-35 (9th Cir. Sep. 15, 2009) (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) <ca9.uscourts.gov/datastore/opinions/2009/09/15/07-17116.pdf>
- *Nosal*, *U.S. v.,* 642 F.3d 781 (9th Cir. Apr. 28, 2011) (in the course of reversing dismissal of an indictment, distinguishing *Brekka* and adopting pro-employer view as to §1030(e)(6)'s "exceeds authorized access" element) <ca9.uscourts.gov/datastore/opinions/2011/04/28/10-10038.pdf>, , *vacated upon grant of rehearing en banc*, 661 F.3d 1180 (9th Cir. Oct. 27, 2011) <http://www.ca9.uscourts.gov/datastore/opinions/2011/11/02/10-10038o.pdf>
- *Rodriguez, U.S. v.,* 628 F.3d 1258, 1263 (11th Cir. Dec. 27, 2010) (distinguishing *Brekka*) <http://www.ca11.uscourts.gov/opinions/ops/200915265.pdf>

District Court Decisions *(alphabetical order)*

- *Alliance Int'l, Inc. v. Todd*, 2008 WL 2859095 (E.D. N.C. July 22, 2008) (pro-employer decision)
- *American Family Mut. Ins. Co. v. Hollander*, 2009 U.S. Dist. LEXIS 16897, *29 (N.D. Iowa Mar. 3, 2009) (when he was an employee, Defendant's access to customer database was "authorized") <https://ecf.iand.uscourts.gov/doc1/0750756276>

U.S. Dist. Ct. Decisions *(c't'd)*

- *Ankersen v. Option Care Enters., Inc.*, 2008 WL 151829, at *11 (S.D. Ind. Jan. 16, 2008) ("'Employee Electronic Information Security Guidelines' . . . [were] summarized in the electronic security agreement . . . . [, which, in turn, wa]s an enforceable contract [that] Plaintiff subsequently violated . . . by copying his Outlook folder, part of Defendant's computer software, and taking that disk with him upon his termination")
- *Arience Builders, Inc. v. Baltes*, 563 F. Supp. 2d 883 (N.D. Ill. 2008) (pro-employer decision)
- *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>
- *Binary Semantics Ltd. v. Minitab, Inc.*, 2008 WL 763575, at *2, *5 (M.D. Pa. Mar. 20, 2008) (finding viable direct claim against Defendant, a competing company, based on Defendant's having induced Plaintiff's employee to steal Plaintiff's trade secrets and come work for Defendant)
- *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 934-36 (W.D. Tenn. 2008) ("*Black & Decker I")* (pro-employee decision based on lack of "unauthorized" element)
- *Bridal Expo, Inc. v. van Florestein*, 2009 WL 255862 (S.D. Tex. Feb. 3, 2009) (pro-employee decision based on lack of "unauthorized" element)
- *B&B Microscopes v. Armogida*, 2007 WL 2814595, *13 (W.D. Pa. Sep. 25, 2007) (though finding that a deletion of files did cause damage and thus violated § 1030(a)(5)(A)(i), also noting that "[t]he CFAA delineates between authorized and unauthorized access; [t]he *Citrin* and *Shurgard* courts' reading of the statute would render this distinction meaningless")
- *Brett Senior & Associates, P.C. v. Fitzgerald*, 2007 WL 2043377, *4 (E.D. Pa. July 13, 2007) (*Lockheed* view inaptly "reads section [1030](a)(4) as if it said 'exceeds authorized use' instead of "exceeds authorized access'"
- *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>
- *Cohen v. Gerson Lehrman Group, Inc.*, No. 09 Civ. 4352 (PKC), 2011 WL 4336683 (S.D.N.Y. Sep. 15, 2011) (denying summary judgment on CFAA claim brought against former employees who modified and deleted data before leaving employment) <http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2009cv04352/345298/165/0.pdf?1316174349>
- *Cohen v. Gulfstream Training Acad., Inc.*, No. 07-60331-CIV, 2008 U.S. Dist. LEXIS 29027, at *12 (S.D. Fla. Apr. 9, 2008) (partially granting summary judgment to employee on his counterclaim; finding "any 'loss' must be related to interruption of service[; i]n this case, the fact that Plaintiff copied files and allegedly stole clients from [his former employer] did not cause an interruption of service as contemplated by the CFAA") <http://www.internetlibrary.com/pdf/Cohen-Gulfstream-SD-Fla.pdf >
- *Condux Int'l, Inc. v. Haugum*, 2008 WL 5244818, *9 (D. Minn. Dec. 15, 2008) (as a matter of law, Plaintiff could not "allege ... 'without authorization' or ... 'exceeded authorized access,' and, thus, the claim for violations of §§ 1030(a)(2), (a)(4), and (a)(5)(ii) and (iii) fail[; moreover,] because there is no allegation of the 'damage' contemplated by the CFAA, the claim for a violation of § 1030(a)(5)(A)(i) likewise fails")

U.S. Dist. Ct. Decisions *(c't'd)*

- *Consulting Prof'l Resources v. Concise Technologies LLC,* 2010 WL 1337723 (W.D. Pa. Mar. 9, 2010) (following *Brekka* 's narrow reading of CFAA as basis for dismissing to claims) <ecf.pawd.uscourts.gov/doc1/15712169362>
- *Del Monte Fresh Produce N.A. Inc v. Chiquita Brands Int'l Inc.*, 2009 U.S. Dist. LEXIS 22694, *10, *21-*23 (N.D. Ill. Mar. 19, 2009) ("copying electronic files from a computer database – even when the ex-employee e-mails those files to a competitor – is not enough to satisfy the damage requirement of the CFAA; there must be destruction or impairment to the integrity of the underlying data;" but finding viable claim against ex-employee for breach of confidentiality provisions of IT Operations Contract) <https://ecf.ilnd.uscourts.gov/doc1/06706222648>
- *Dental Health Products, Inc. v. Ringo*, No. 08–C–1039, 2011 WL 3793961 (E.D. Wis. Aug. 25, 2011) (granting summary judgment for plaintiff on CFAA claim based on defendant's copying information before leaving employment) <http://docs.justia.com/cases/federal/district-courts/wisconsin/wiedce/1:2008cv01039/48584/155/0.pdf?ts=1314369676>
- *Diamond Power Int'l, Inc. v. Davidson*, 2007 WL 2904119, at *14 (N.D. Ga. Oct. 1, 2007) ("the phrase 'without authorization' generally only reaches conduct by outsiders who do not have permission to access the plaintiff's computer in the first place. . . . Stated differently, a violation does not depend upon the defendant's unauthorized use of *information*, but rather upon the defendant's unauthorized use of *access*") <https://ecf.gand.uscourts.gov/doc1/05502250205>
- *Ennis Transp. Co. Inc. v. Richter,* 2009 WL 464979 *1-*2 (N.D. Tex. Feb. 24, 2009) (loss duly alleged in Complaint's allegations that ex-employees exceeded authorized access by "utiliz[ing" confidential information obtained from . . . [employer's] contracts, customer lists, schedules [and] employee files . . . to steal business") <https://ecf.txnd.uscourts.gov/doc1/17704261799>
- *Ervin & Smith Advertising and Public Relations, Inc. v. Ervin*, 2009 WL 249998 (D. Neb. Feb. 3, 2009) (pro-employer decision) <https://ecf.ned.uscourts.gov/doc1/11301655270>
- *Facebook, Inc. v. MaxBounty, Inc.*, No. 5:10-cv-04712-JF (HRL), 2011 WL 4346514 (N.D. Cal. Sep. 14, 2011) (denying motion to dismiss CFAA claim based on access to Facebook in violation of Facebook's terms of service) <http://docs.justia.com/cases/federal/district-courts/california/candce/5:2010cv04712/233063/46/0.pdf?1316081987>
- *Farmers Bank & Trust v. Witthuhn*, No. 11-2011-JAR, 2011 WL 4857926 (D. Kan. Oct. 13, 2011) (denying motion to dismiss CFAA claim where reasonable jury could find employer's information security policy could mean defendant exceeded authorized access) <https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2011cv2011-94>
- *Fink v. Time Warner Cable*, --- F.Supp.2d ----, 2011 WL 3962607 (S.D.N.Y. Sep. 7, 2011) (denying motion to dismiss because the changing nature of technology requires a broad reading of access and authorization) <http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2008cv09628/335276/64/0.pdf?1315484558>
- *First Mortgage Corp. v. Baser*, 2008 WL 4534124, at *2 (N.D. Ill. Apr. 30, 2008) (whether ex-employee exceeded authorized access was a fact question, as to which ex-employer was entitled to discovery so as to defend against summary judgment motion)
- *Fontana v. Corry*, No. 10–1685, 2011 WL 4473285 (W.D. Pa. Aug. 30, 2011) (holding plaintiff alleged access exceeding authorization where defendant was granted access to certain accounts, but in fact accessed and transferred money from other accounts) <ecf.pawd.uscourts.gov/doc1/15712879792>, as adopted by 2011 WL 4461313 (Sep. 26, 2011) <docs.justia.com/cases/federal/district-courts/pennsylvania/pawdce/2:2010cv01685/194660/11/0.pdf?ts=1317128656>

U.S. Dist. Ct. Decisions *(c't'd)*

- *Forge Indus, Staffing v. De La Fuente*, 2006 WL 2982139, at *6 (N.D. Ill. Oct. 16, 2006) (declining to follow *Citrin*'s interpretation of the CFAA's "without authorization" and "exceeding authorization" terminology) <http://Forge-DeLaFuente-NDIll-10-16-06.notlong.com>
- *Garelli Wong & Assocs., Inc. v. Nichols*, 2008 WL 161790, at * 7 (N.D. Ill. Jan. 16, 2008) (not addressing "exceeded authorized access" element; instead dismissing because "where a trade secret has been misappropriated through the use of a computer, we do not believe that such conduct alone can show 'impairment to the integrity or availability of data, a program, a system, or information[' under] 18 U.S.C. § 1030(e)(8)") <https://ecf.ilnd.uscourts.gov/doc1/06702343965>
- *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 10-1029, 2011 WL 4467767 (E.D. Pa. Sep. 23, 2011) (noting lack of contract meant plaintiff could not plead defendant exceeded authorized access) <paed.uscourts.gov/documents/opinions/11D1074P.pdf>
- *Hasan v. Foley & Lardner, LLP*, 2007 U.S. Dist. LEXIS 54930, at *13 (N.D. Ill. July 26, 2007) (distinguishing *Citrin*, in that, here, employer introduced "no evidence, through expert testimony or otherwise, that [former employee actually] intentionally caused any damage by deleting even a single file with Internet Washer Pro" program on laptop before returning it to employer) <http://Hasan-Foley-NDIll-7-26-07.notlong.com>
- *Hewlett-Packard Co. v. Byd:sign, Inc.*, 2007 WL 275476 at *13 (E.D. Tex. Jan. 25, 2007) (upholding viability of employer's CFAA claim against disloyal former employees, focusing on company policies – in which, according to Complaint, "Defendants had agreed not only to refrain from disclosing information, but also to refrain from sending or accessing messages on [Plaintiff-employer]'s computer systems for personal gain") <https://ecf.txed.uscourts.gov/doc1/17501170446>
- *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005) ("Plaintiff simply cannot overcome the fact, supported by its own allegations, that [secretary-treasurer of local unit of labor union] was authorized to access the information . . . , and that at the time she was allegedly accessing it on behalf of [a rival union], her access had not been revoked.") <http://IAM-Werner.notlong.com>
- *Jarosch v. American Family Mutual Insurance Co.*, No. 07-C-0212, 2011 WL 4356346 (E.D. Wis. Sep. 16, 2011) (holding former insurance agents accessed insurance companies' files without authorization because the agents had already planned to start competing business) <http://docs.justia.com/cases/federal/district-courts/wisconsin/wiedce/2:2007cv00212/43000/202/0.pdf>
- *Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing, & Consulting, LLC*, 2009 WL 151687, *6 (E.D. Mo. Jan. 22, 2009) (dismissing CFAA-related counts because Plaintiff failed to properly allege "without authorization;" citing above *Condux* decision) <https://ecf.moed.uscourts.gov/doc1/10702616802>
- *Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. LEXIS 53108, at *11-25 (M.D. Fla. Aug. 1, 2006) <http://Lockheed-Speed-8-01-06.notlong.com> (employees' copying of computer files before departing for a rival firm was neither "without authorization" nor "exceeding authorization" – because such access had occurred while employees had still enjoyed access rights to the company's computer system)
- *LKQ Corp. v. Thrasher*, 785 F. Supp. 2d 737 (N.D. Ill. May 23, 2011) (denying dismissal because former employer alleged breach of loyalty by former employee) <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2011cv02743/254901/23/0.pdf?1306234982 >

U.S. Dist. Ct. Decisions *(c't'd)*

- *Marine Turbo Engineering, Ltd. v. Turbocharger Services Worldwide, LLC*, 2011 WL 6756916 (S.D. Fla. Dec. 22, 2011) (denying motion to dismiss CFAA claim based on violation of employment contract) <http://docs.justia.com/cases/federal/district-courts/florida/flsdce/0:2011cv60621/375992/207/0.pdf?ts=1324644210>
- *Mintel Int'l Group, Ltd. v. Neergheen*, 2008 WL 2782818, at *3 (N.D. Ill. Jul. 16, 2008) ("exceeded authorized access" allegations sufficient to show likelihood of success justifying TRO)
- *MPC Containment Systems, Ltd. v. Moreland*, 2008 WL 2875007 (N.D. Ill. Jul. 23, 2008) (pro-employer)
- *Modis, Inc. v. Bardelli*, 2008 WL 191204, at *3-5 (D. Conn. Jan. 22, 2008) (though dismissing without prejudice due to lack of specificity as to nature of requisite damage, finding that "exceed[ed] authorized access" element *was* shown – by virtue of employment agreement's general prohibition on taking or using any company property except in furtherance of company business) <https://ecf.ctd.uscourts.gov/doc1/04101606517>
- *Motorola Inc. v. Lemko Corp.*, 2009 U.S. Dist. LEXIS 10668, *14-*16, *18-*19, *22-*23 (N.D. Ill. Feb. 11, 2009) (citing the above *Mintel* decision, finding allegations that an employee e-mailed and downloaded confidential information for an improper purpose sufficient to state claim that employee exceeded her authorization) <https://ecf.ilnd.uscourts.gov/doc1/06706071965>
- *Nilfisk-Advance v. Mitchell*, 2006 US Dist. LEXIS 21993 (W.D. Ark. Mar. 28, 2006) (denying ex-employee's motion to dismiss based on employee having exceeded authorization once he had developed intent to misappropriate trade secrets) <https://ecf.arwd.uscourts.gov/cgi-bin/show_case_doc?13,26525,,,,,52,1>
- *P.C. of Yonkers, Inc. v. Celebrations! The Party And Seasonal Superstore, L.L.C.*, 2007 WL 708978, at *4-7 (D.N.J. Mar. 5, 2007) (in course of denying motions to dismiss CFAA claims and related state law claims against former employees, apparently assuming impropriety of access to company information used to fraudulently develop business directly competitive with employer) <http://PCYonkers-Celebrations.notlong.com>
- *Patrick Patterson Custom Homes Inc. v. Bach*, 586 F. Supp. 2d 1026, 1034-35 (N.D. Ill. Nov. 14, 2008) (denying 12(b)(6) and 9(b) motion to dismiss where Plaintiff alleged ex-employee had "intentionally accessed their protected computer in a manner which exceeded her authority" not only by embezzling funds via making electronic fund transfers to herself and to her personal creditors but also by "delet[ing] various files . . . and caus[ing] a 'shredding' software to be installed . . . to destroy the computer files and render them unrecoverable") <https://ecf.ilnd.uscourts.gov/doc1/06705742505
- *Resource Ctr. For Independent Living, Inc. v. Ability Resources, Inc.*, 534 F. Supp. 2d 1204, 1211 (D. Kan. 2008) ("the restrictive view of 'authorization' [was to be] adopted. . . . Here, [the former employee] was authorized to initially access the computer he used. . . . [Thus, he] did not access the information at issue 'without authorization' or in a manner that 'exceed[ed] authorized access.'")
- *Sam's Wines & Liquors, Inc. v. Hartig*, 2008 WL 4394962, at *3 (N.D. Ill. Sep. 24, 2008) (though following *Citrin* on the "exceeded authorized access" element, dismissing Complaint because Plaintiff had "failed to properly plead damage under the CFAA")
- *Seal Source, Inc. v. Calderon*, No. 03:09-CV-00875-HU, 2011 WL 5041275 (D. Or. Sep. 29, 2011) (denying summary judgment for defendant on CFAA claim based on disputed issue whether defendant exceeded his authorized access under his employment contract) <https://ecf.ord.uscourts.gov/doc1/15113896093>, *as adopted* by 2011 WL 5057079 (D. Or. Oct. 24, 2011) <http://docs.justia.com/cases/federal/district-courts/oregon/ordce/3:2009cv00875/93922/102/0.pdf>

U.S. Dist. Ct. Decisions *(c't'd)*

- *Secureinfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 609-10 (E.D. Va. 2005) (dismissing claim in case outside employer/employee context) <http://Secure-Telos.notlong.com>
- *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967-68 (D. Ariz. 2008) (certifying interlocutory appeal, asking the Sixth Circuit to provide guidance in the uncertain context of the "unauthorized" element; "[f]urther, [the employer] conceded that [the employee] was permitted to view the specific files he allegedly emailed to himself")
- *SKF USA, Inc. v. Bjerkness*, No. 08 C 4709, 2009 U.S. Dist. LEXIS 34781, at * 57 (N.D. Ill. Apr. 24, 2009) (dismissing CFAA claim because "[p]urely economic harm unrelated to the computer systems is not covered by" pertinent statutory definition)
- *Statera, Inc. v. Hendricksen*, Ex Parte TRO, 2009 WL 2169235 (D. Colo. July 17, 2009), extended for 60 days by stipulation in TRO, 2009 WL 2358934 (D. Colo. July 20, 2009) (TRO based on likelihood of success on merits of ex-employer's CFAA claims)
- *U.S. Bioservs. v. Lugo*, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009) ("follow[ing] the line of cases that have rejected a reading of the CFAA by which the defendant's intent may determine whether he has acted without authorization or has exceeded his authorized access") <https://ecf.ksd.uscourts.gov/doc1/07901821346>
- *Wells Fargo Bank, N.A. v. Clark*, No. CIV. 11-6248-TC, 2011 WL 3715116 (D. Or. Aug. 23, 2011) (granting preliminary injunction for Wells Fargo based on allegations Clark returned his work laptop late and damaged) <http://docs.justia.com/cases/federal/district-courts/oregon/ordce/6:2011cv06248/103693/23/0.pdf?ts=1314190493>
- *Wentworth-Douglas Hosp. v. Young & Novis Prof'l Ass'n*, 2010 WL 3023331, at *3 (D. N.H. July 28, 2010) (denying motion to dismiss) <http://op.bna.com/hl.nsf/id/psts-87uq45/$File/went.pdf>
- *Winner, Inc v. Polistina*, Civil Action No. 06-4865, 2007 U.S. Dist. LEXIS 40741 (D.N.J. June 4, 2007) (CFAA does not permit a private cause of action based merely on an employee's misuse of the employer's email system) <https://ecf.njd.uscourts.gov/doc1/1190797820>
- *Zero Down Supply Chain Solutions, Inc. v. Global Transportation Solutions, Inc.*, 2008 WL 4642975 (Oct. 17, 2008) (denying 12(b)(6) and 9(b) motion to dismiss; under Fed. R. Civ. P. 8(a), sufficient allegations included that former employees and their co-conspirator had: "accessed Plaintiffs' online bank account, changed the user name and password, ... obtained and falsely manipulated financial information ... used to divert Plaintiffs' assets[,] ... obtained Plaintiffs' confidential financial and business information, and installed ... two malicious software programs ... allow[ing] remote access")

State Court Decisions as to CFAA and/or State Analogues

- **N.J.:** *State v. Riley*, 412 N.J. Super. 162, 988 A.2d 1252, 1267 (in applying New Jersey's computer crime law, "find[ing] persuasive those decisions that adhere to the narrow interpretation of the federal prohibition of access without or exceeding authorization.") (Oct. 30, 2009) <caselaw.findlaw.com/nj-superior-court/1508996.html>
- **N.Y.:** *Hecht v. Components Int'l. Inc.*, 22 Misc. 3d 360, 867 N.Y.S. 2d 889, 898 (N.Y. Sup. Nassau Cty. Nov. 6, 2008) (granting summary judgment in favor of a former employee, where Plaintiff had not demonstrated "intent to defraud" in that there had been no accessing of "sensitive information") <http://decisions.courts.state.ny.us/10JD/Nassau/decisions/INDEX/INDEX_new/AUSTIN/2008NOV/003371-08.pdf>

APPENDIX E – Robert D. Brownstone – Social-Media Ethics – Lawyers, Jurors & Judges – Partial Bibliography (@ 2/16/12)

1. Lawyers

- **Exposing Client Confidences, Conflicts of Interest, etc.**
  - *Ethical Pitfalls*" – three-part series by Quarles & Brady:
    - 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 (9/15/11) <html.documation.com/cds/SBC2011/HTML%20Files/PDFs/014.pdf>
- **"Friend"-ing Witnesses and/or Represented Parties**
  - San Diego Cty. Bar Ass'n, *Legal Ethics Opinion 2011-2* (5/24/11) <http://www.sdcba.org/index.cfm?pg=LEC2011-2>
  - NYSBA Comm. On Prof'l Ethics, *Op. # 843* (9/10/10) <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>

2. Jurors

- Eva-Marie Ayala, *Tarrant County juror sentenced to community service for trying to 'friend' defendant on Facebook*, Ft. Worth Star-Telegram (8/28/11) <http://www.star-telegram.com/2011/08/28/v-print/3319796/juror-sentenced-to-community-service.html>
- *Cal. A.B. 141* (signed by Gov. Brown 8/5/11) <www.leginfo.ca.gov/cgi-bin/postquery?bill_number=ab_141&sess=CUR&house=B&author=fuentes>
- Judge Linda F. Giles, *Does Justice Go Off Track When Jurors Go Online?* 55 Boston Bar. J. No. 2, at 7-9 (3/21/11) <www.bostonbar.org/pub/bbj/bbj_online/bbj1011/spring2011/bbj_spring2011.pdf#page=7>
- Compare Brian Grow, *Internet v. Courts: Googling for the perfect juror*, Reuters Legal (2/17/11) <http://www.reuters.com/article/2011/02/17/us-courts-voirdire-idUSTRE71G4VW20110217>

3. Judges

- Okla. Judicial Ethics Advisory Panel, *Judicial Ethics Op. 2011-3* (7/6/11) <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* (12/3/10) <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* (1/20/10) <http://courts.ky.gov/NR/rdonlyres/FA22C251-1987-4AD9-999B-A326794CD62E/0/JE119.pdf>
- Fla. Sup. Ct. Judicial Ethics Advisory Comm., *Op. No. 2009-20* (11/17/09) <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 network-ing 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* (1/29/09) <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 (4/1/09) <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 (9/2/11) <http://volokh.com/2011/09/02/may-judges-be-facebook-friends-with-lawyers-or-others-who-regularly-appear-before-them/>
- J. Randolph Evans and Joshua B. Belinfante, *Ga. Judges on Facebook: To Friend or Not to Friend?*, Fulton Cty. Daily Report (8/30/11) <www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202512740798>
- Terry Baynes, *Would You 'Friend' the Judge?* (Am. Lawyer 10/26/10) <http://web.archive.org/web/20101101233344/http:/www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202473899448>
- 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/>

Appendix F

NELI ELB

March 2012

Miami, FL &

San Diego, CA

The eWorkplace – Technology-Use, Social-Media & Privacy 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 & BACKGROUND CHECKS**
  - *Following the Internet Trail; Credit Checks*
- **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 additional concerns:**
  - **Ever-expanding universe of forums**
  - **MANY more ways to expose information**
  - **Everyone can be a publisher**
  - **Personnel matters play out in public**

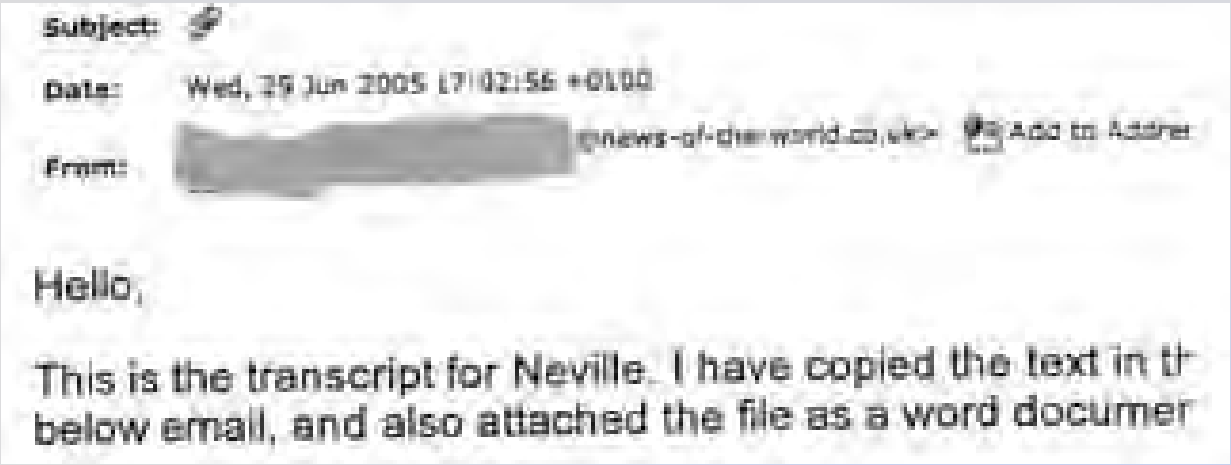
I(A). INTRO *(c't'd)* – Liability Risks & Data Leakage

- ***Unintentional*** **Loss or Theft of Sensitive Information**
- ***Inadvertently*** **Harmful Intentional Disclosures ("Netiquette," Social-Media, etc.)**
- ***Intentionally*** **Harmful Intentional Disclosures**

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**

I(B)(1). Smoking Guns – Murdoch *(c't'd)*



Subject:

Date: Wed, 29 Jun 2005 17:02:56 +0100

From: [redacted]@news-of-the-world.co.uk> Add to Addres

Hello,

This is the transcript for Neville. I have copied the text in th below email, and also attached the file as a word documer

An email sent by Ross Hall from the News of the World to private investigator Glenn Mulcaire

- **So far . . . 58 settlements**
- **$15.8 M in USD**
- **6 more cases filed; 50 more anticipated**
  - **Lisa O'Carroll and Dan Sabbagh, *News International pays out but faces further phone-hacking claims*, UK Guardian (2/8/12)**

I(B)(1). Liability Evidence – Smartphones Too

- "*Textual harassment*"
- ***And* . . . search-incident-to-lawful-arrest**
  - *People v. Diaz*, **244 P.3d 501 (Cal. 1/3/11)**
  - ***But* see pending Cal. legislation:**
    - **SB 914 Status Page (vetoed 10/9; back to Senate)**
    - **SB 914 Text**
    - **Perry L. Segal, e-Discovery California: *The 'Leno' Show Seeks to Overturn Diaz: SB 914*, e-Discovery Insights (6/17/11)**
- ***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)**

I(B)(1). Smartphones Too *(c't'd)* . . .

http://www.product-reviews.net/2011/10/19/iphone-4s-find-my-friends-app-catches-cheating-wife/

- ***"Your Cheating Heart: iPhone App Finds Wife With Another Man"***
  - **Ned Potter, ABC News (10/17/11)**

- ***"You Know Who Really Loves Smartphones? Divorce Lawyers."***
  - **Ina Fried, *All Things Digital* (2/8/12)**

I(B)(1). Smartphones Too *(c't'd)* . . .

- **And there's still the web . . .**
- **"Semi-Naked Came the Congressman"**
  - **Gail Collins, NYT Op-Ed (2/12/11)**

" Will someone prove to me not all [Craig's List] men look like toads?" . . . .

"Hi . . . Hope I'm not a toad . . . . "I'm a very fit fun classy guy . . . . Live in Cap Hill area . . . . 39-year-old lobbyist . . . . I promise not to disappoint."

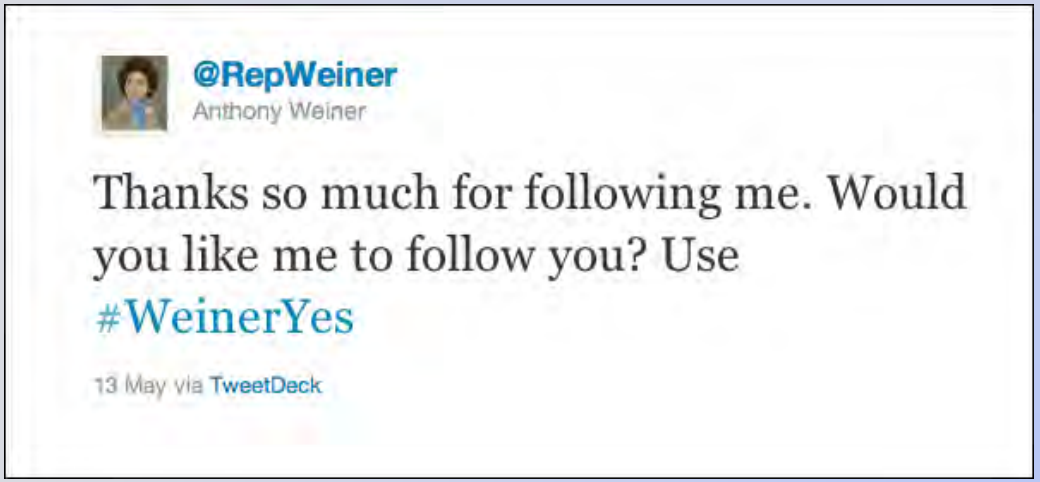
- **46 year old (now-ex) Congress-person Christopher Lee**
- ***New York Congressman Resigns Over Shirtless Photo*, NYT (2/10/11)**

I(B)(1). Smartphones Too *(c't'd)* . . .

- **Ex-Congressperson Anthony Weiner**

  - **Steven Levy, *How Early Twitter Decisions Anthony Weiner's Dickish Demise***

<www.wired.com/epicenter/2011/06/twitter-follow-weiner-dickish/all/1>



- **Ex-Sen. in PR Legislature (& ex-Progressive Party Pres.) Robert Arango grindr images**
  - **RT, *Anti-gay Senator caught on all-gay dating site* (8/29/11)**

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

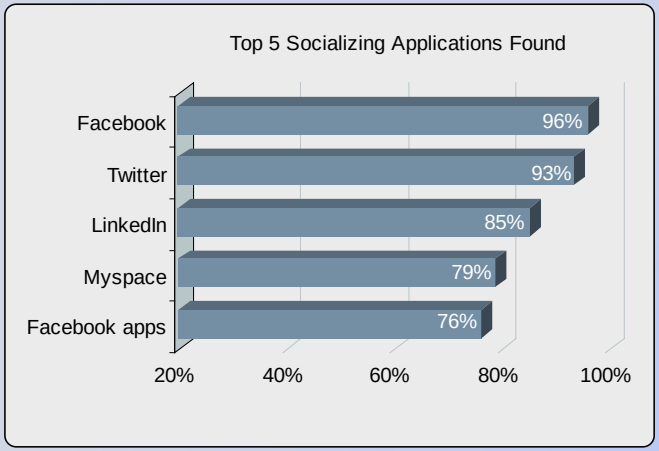
I(B)(2). Web 2.0 – "Saying, Socializing & Sharing"

paloalto NETWORKS
the network security company™

* Also a client

- **Facebook surpassed Google in user minutes in August 2010. *See* footnote 29 in Paper.**
  - **PAN, *Application Usage and Risk Reports* (Oct. '10 & May '11)**

    <http://www.paloaltonetworks.com/researchcenter/reports/> . . .



- **Facebook most used site OF ANY SORT @ May '11**
  - **Nielsen, *Social Media Report Q3 2011* (9/8/11)**

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

- ***PROS:***
  - **Per Oct. '10 PAN Report (cited in Slide 11 above):**
    - **Responsiveness**
    - **Rich research**
    - **PR**
  - **Transparency**
  - **Networking**
- ***For slides / links re: Success Stories, contact Presenter***

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

- ***PROS***
- **Tech toolbox has grown:**
  - **Teneros' *Social Sentry* enables employers to look at employee's public posts**

    <http://bits.blogs.nytimes.com/2010/03/26/keeping-a-closer-eye-on-workers-social-networking/>
  - **PAN firewalls can switch Facebook to read-only**

    <http://www.readwriteweb.com/enterprise/2010/06/read-only-facebook-coming-to-y.php>

    <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/10/23/BULH1LKCDV.DTL&type=printable>

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

- ***CONS:***
  - **INCOMING! and . . . OUTBOUND!**

  - **Kashmir Hill, *You May Not Want To Check Facebook At Work Today*, Forbes (11/15/11)**
  - ***See generally this list and that list***

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

- ***CONS*** *(c't'd)*:
  - **Every Post Can Last Forever**
  - **Search-ability**
  - **Capture-ability**
    - ***See, e.g.,*** **"*Would you Friend the Judge?*" (linking to iCyte & PageFreezer)**
  - **Wayback Machine**
  - **Tweets are especially persistent**

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

- **A generic concern – sock-puppeting (pseudonymous/anonymous postings)**
  - **FTC endorsement/testimonial rules**
  - **Securities laws**
  - **Antitrust laws**
- **Some industry-specific concerns:**
  - **FDA**
  - **FINRA**
- ***See* resources linked in footnotes 36-38**

I(B)(2). Social-Media – Privacy?!

- **Discretion?! . . .**
  - **"You never talk in a club, you never talk in a car, you never talk on a cell phone, you never talk on a phone, you never talk in your house. You go on a walk-talk - I don't know anybody who was ever locked up or arrested for a walk-talk."**
    - **JOSEPH C. MASSINO, the longtime boss of the Bonanno crime family, testifying in United States District Court in Brooklyn.**
      - ***William K. Rashbaum,* *A Mafia Boss Breaks a Code in Telling All*, NYT (4/12/11)**

I(B)(2). Social-Media – Privacy?! *(c't'd)*

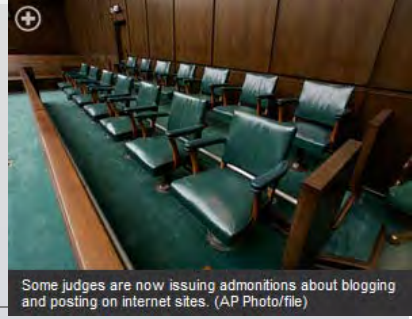
MISTAKEN IDENTITY

- **TAG . . . . You're it . . . .**

I(B)(2). Social-Media Privacy? Photo/Video Tags *(c't'd)*

- **Recent developments:**
  - **Facebook settings have changed**
    - **Facebook, *Making It Easier to Share With Who[m] You Want* (8/23/11)**
  - **EU countries' probes of tag-ging and facial recognition**
  - **But, in U.S., one court – in a divorce/custody case – OK'd tags**
    - ***Lalonde v. Lalonde*, No. 2009-CA-002279-MR (Ky. Ct. App. 2/25/11)**
- ***See* footnote 46 of Paper for more re: these developments**

I(B)(2). Social-Media – Privacy?! *(c't'd)*


Some judges are now issuing admonitions about blogging and posting on internet sites. (AP Photo/file)

- **Recent developments *(c't'd)*:**
  - **Ethics / sanctions developments re: lawyers, jurors & judges . . .**
    - **Appendix E**
  - **U.S. Navy Slideshare, *What's the deal with Google+?* (7/29/11)**

I(B)(2). eDiscovery Decisions

- **Case-law has been emerging**
  - **See Appendix B**
  - ***See my "button" example***
- **Intranet sites: [quoting me ☺]:**
  - ***Yammer, Chatter, Hot Water*, BusinessWeek (4/28/11)**

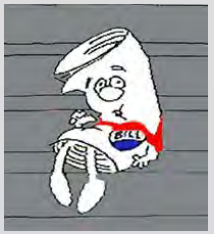
II. Monitoring – Risk-Management Justifications

- **REMEMBER 3 Types of Concerns, e.g., . . .**
- **Maintain and track workers' activities productivity and locations**
- **Network security**

II. Web 2.0 Risks *(c't'd)* – Intentional Conduct

- One key issue = (ostensible) authority to speak on behalf of gov't re: work-related matter
- Also: Direct misuse of confidential information to harm (ex-)employer

II. Monitoring – Justifications



- **Protecting Individuals' Personally Identifiable Information (PII):**
  - **States' notice-of-breach and other anti-identity-theft statutes**
    - <www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>
  - **> 40 apply to private sector**
  - **≥ 13 of those apply to public sector too (Alaska, Cal., DC. Ill., Ind., Md., Mich., NC, NY, NJ, Nevada, OK, Wash.)**

II. Monitoring – Risk-Mgmt. Justifications

- **Direct claims based on leaks and/or breaches**
  - ***Wikileaks* (250,000 cables)**
    - **ALL eventually made public by Wikileaks itself (9/2/11)**
  - ***Krottner v. Starbucks* (9th Cir. 12/14/10) (2 decisions)**
- **Third parties' claims (*e.g.*, libel, harassment) based on employee's conduct/postings**

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 Op. Co.*, 130 S. Ct. 2619 (6/17/10)** <www.supremecourt.gov/opinions/09pdf/08-1332.pdf>
  - ***See* pp. 20-25 of Paper, incl. Top Ten Tips**

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

- ***Aside from SOME 1st and 4th Amendment claims*, typically courts support employer**
- **BUT 2 potential exceptions even in private sector case law:**
  - **examining locally-stored files impinging on an employee's attorney-client (a/c) privilege; OR**
  - **illicitly obtaining password and accessing content in personal account or site**

II. Privacy Expectations – A/C Privilege – Split *(c't'd)*

- **ONE RECENT DECISION:**
  - ***Holmes v. Petrovich*** **(Cal. App. 3 Dist. 1/13/11)**
- **OTHER DECISIONS/ARTICLES:**
  - **Appendix C**
- ***PRACTICAL TIPS***
  - **Policy language**
  - **Investigation protocol**

II. Expectations *(c't'd)* – ECPA Intrusions

- **Avoid unauthorized intrusions into employees' personal Web 2.0 pages, passwords or e-mail**
- **Violates ECPA Title I (Wiretap) or Title II (SCA)**

II. Expectations *(c't'd)* – ECPA Intrusions *(c't'd)*

- **BUT SEE this recent state court case:**
  - **Employee's own computer:**
    - **physically in a workplace office**
    - **connected to the employer's network**
    - **displaying a way to get to personal webmail**
  - **Employee suspected of engaging in competing co.**
  - **Webmail accessed and printed = OK under policy's broad investigation rights**
  - **Affirmed: judgment for employer dismissing common law and state statutory invasion claims**

Sitton v. Print Direction **(Ga. App. 9/28/11)**

II. Another Concern – Union Activity

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

- **Lots of NLRB Activity**
  - ***For NLRB GC Reports*, complaints, settlements & decisions (INCLUDING 1/24/12 Report), *see* pp. 32-35 & 57-60 of Paper**
- **Compare, *e.g.*, these two '11 ALJ decisions . . .**
  - ***Knauz* (sales-event criticisms & accident-photos)**
  - ***Hispanics United* (criticisms of co-worker)**
- **. . . with '11 GC Advice Memo in *Lee/Arizona***

II. NLRB Activity *(c't'd)*

NATIONAL LABOR RELATIONS BOARD

- **Takeaways?**

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

- **Avoid fine distinctions as to prohibitions?**
- **Track rejections of personal use?**
- **Add "concerted action" in "savings" clause? (without "chilling" or "intimidating" . . . ??)**

III. Investigations and Background Checks

- **Distinguish . . .**
- ***Criminal history*** **(*e.g.*, Mass. CORI statutes)**
  - **Adam Klein Written Testimony, *Computer-Database Background Investigations, Criminal Records, and Hiring Discrimination*, Meeting of July 26, 2011 – EEOC to Examine Arrest and Conviction Records as a Hiring Barrier <www.eeoc.gov/eeoc/meetings/7-26-11/klein.cfm>**
    - ***Citing Johnson v. Locke*, 10 Civ. 3105 (S.D.N.Y.)**
      - **For First Amended Complaint (8/5/10), click *here***
- **For public-sector decision/reversal, *see* *Nelson v. NASA*, 1131 S. Ct. 746 (1/19/11) (questions in civil service questionnaire re: illegal-drug use) <www.supremecourt.gov/opinions/10pdf/09-530.pdf>**

III. Investigations & Background Checks

- ***Credit report information*** **(FCRA/FACTA & State Analogues) re: whole lifecycle**
  - ***FTC Testifies on the Rights of Employees Under the Fair Credit Reporting Act*** **(10/20/10)**

    <www.ftc.gov/opa/2010/10/faircredit.shtm> (linking to <ftc.gov/os/testimony/101020eeoctestimony.pdf>)
- **Note bans passed by Oregon, Hawaii, Washington – and California (AB 22 effective 1/1/12) as well as much other contemplated legislation**

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

Social Intelligence℠

- **Kashmir Hill, *Feds Okay Start-up That Monitors Employees' [AND APPLICANTS'] Internet and Social Media Footprints*, Forbes (6/15/11)**

- **Social Intelligence – "Monitoring" and "Hiring" solutions . . . .**

FCRA CONSUMER RIGHTS ATTACHED

COMPANY:

ADDRESS: 735 State Street
Santa Barbara, CA 93101

COMPLETED REPORT

PHONE: (888) 748-3281

FAX: (805) 413-2036

Social Intelligence

Social Media Consumer Report

APPLICANT: Leonard

EMAIL ADDRESS:

ORDERED: 01/26/2011

COMPLETED: 01/26/2011

REPORT SUMMARY

REPORT TYPE: Social Media Verification

CLASSIFICATION: Negative

MATCH CRITERIA: Demonstrating potentially violent behavior

SUB-FILTER: Flagrant display of weapons or bombs

SOURCE: http://hi5.com/112121

MATCHED BY: First and Last Name, Email Address

COMMENTS: Subject is holding assault rifle, with other individuals brandishing a handgun and a sword, while consuming an alcoholic beverage

HIGHLIGHTED IMAGE

SIC provides the information contained in this report to End-User to be used solely for a permissible employment purpose as defined in the Fair Credit Reporting Act. If the End-User intends to take adverse action based in whole or in part on the contents of this report, the End-User must provide the consumer with notices that it is taking adverse action and those notices must comply with the FCRA and state law. All information contained in this report is provided pursuant to the terms of the End-User Agreement. End-User further understands that it uses any and all information provided by CIA at its own risk and End-User is solely liable for complying with all federal, state, and local laws.

The information contained in this report is confidential and may only be accessed by authorized employees of End-User, provided to the consumer about who it relates, or provided as otherwise required by law.

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

Federal Trade Commission
Protecting America's Consumers

- ***But see* FTC concerns re: marketers of background-screening Mobile Apps**
  - FTC Press Release Linking to 3 Warning Letters re: "consumer reporting agency" (2/7/12)
    - **Irony: last sentence of Release: "Like the FTC on Facebook and follow us on Twitter."**
  - Fenwick & West Article re: same (2/15/12) **[LINK CORRECTED]**

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

- **Following Applicant's Internet Trail**
  - **Weak "expectation of privacy" claim**
  - **Traditional labor law concepts**
  - **For barometer re: employers' HR approaches as to applicants, *see* footnotes 163-69, at pp. 39-40, of Paper**
- **What about asking applicant for:**
  - **Twitter name or Facebook URL to view public posts?**
  - **FB login & password to view all content (incl. private)?**
    - **Ex: Md. state agency situation at footnotes 62, 85 and 169 of Paper [NOTE: agency backed down after ACLU threat]**
    - **NEW: forced shoulder-surfing in private sector as discussed in Time, threatpost and also this Time article**

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
J[redacted] M[redacted]

Children:
J[redacted] M[redacted]
J[redacted] M[redacted]

Information

Political Views:
demo 4 insight

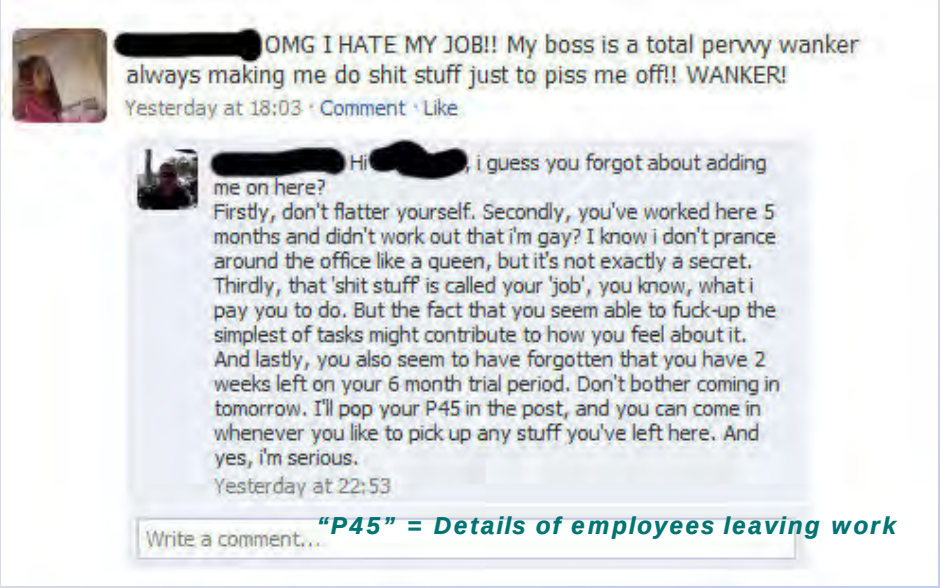
Religious Views:
buish or jewbu

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

- **State statutory protections too, of course**
- **What could go wrong? Exs:**
  - **Loose lips . . . OR . . . .**
  - **"MODERN ASTRONOMY, THE BIBLE, AND CREATION" – Title VII claim based on Applicant's alleged creationist views coming to light based on web searching during hiring process for astronomy observatory director**
    - ***Gaskell v. Univ. of Ky.*, 2010 WL 4867630 (E.D. Ky. 11/23/10)**

      <media.aclj.org/pdf/gaskell_summary_judgment_order_20101206.pdf>

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

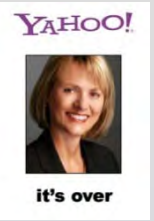


"P45" = Details of employees leaving work

- **Zee, *Note to self: Don't 'friend' your boss on FB and then bitch about your job*, The Next Web (8/9/09)**
- ***See also* <http://www.lamebook.com/fired-via-facebook/>**
- ***Compare "no unlawful surveillance if ... 'friended' . . . Supervisor" (pp. 33-34 of latest NLRB GC Report)***

- **Should management response be online?**
  - ***Ex.: Wash. Post Suspends Columnist for Twitter Hoax***

IV. "Off-Duty"? – Stupid Employee Tricks *(c't'd)*



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

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

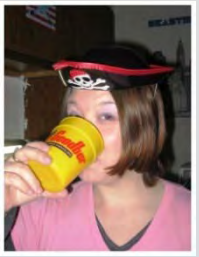
- ***See also* David Streitfeld, *Blunt E-Mail Raises Issues Over Firing at Yahoo*, N.Y. Times (Sep. 7, 2011)**

- **. . . and these:**
  - **Christine Harper, *Goldman Stunned 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*, SF Chron (3/16/12) (Google & Yahoo too . . .)**

IV. Looking Into "Off-Duty" Activities

- **Employee caught in compromising post(s) when "out sick" or on leave**
- **State statutes apply**
- **At least for pub. employees, so do codes of conduct and policies**
- **More severe (indecent) conduct, especially by a public employee?**
  - **Ex: *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)**

IV. Looking Into "Off-Duty" Activities



- **Remember the Drunken Pirate?**
- **NEW! What about statutes restricting teacher-student Internet contact?**
  - **As to Missouri situation, *see* page 46 of Paper**
- **In general in private sector, traditional rules presumably still apply.**

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

- **BUT there are always other new topics/questions . . .**
  - **Social-media check-ins by an employee . . . ?**
    - **ACLU dotrights, *Location-Based Services Privacy Check-In* (11/16/10)**
  - **What if boss or HR not "friend-ed" but receives a forward or a print-out from someone who is a friend? . . .**
    - **See various examples in recent NLRB GC Report**

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

- **"Who Owns a Terminated Employee's Twitter Account?"**
  - **Bruce Carton, Legal Blog Watch (10/4/10) (CNN's Rick Sanchez) <http://legalblogwatch.typepad.com/legal_blog_watch/2010/10/who-owns-a-terminated-employees-twitter-account.html>**
- **"As rolodexes go online ownership is muddy"**
  - **Brian Sumers, D.J. (11/9/10) (citing *Sasqua Group, Inc. v. Courtney*, 2010 WL 3613855 (E.D.N.Y. 8/2/10) (availability of LinkedIn), *as adopted by* 2010 WL 3702468 (9/7/10); *TEKSystems Inc. v. Hammernick*, Complaint, No. 10-00819 (3/6/10) (use of LinkedIn to contact people))**
- **"Is social media entitled to trade secret protection?"**
  - **Eric Syverson, D.J. (2/3/12) (policy tips; some VERY unrealistic) (citing *PhoneDog v. Kravitz*, No. C 11-03474 (N.D. Cal. 2012) (all company's Twitter passwords allegedly "confidential information"), eDocket available at this link**

V. Compliance Basics

Let the Harmony Begin

TOSHIBA
Dont copy. Lead.®

- **KUMBAYA?!**

- **Clear, well-thought-out language on which multiple constituencies have weighed in . . .**
- **Compliance's "3 E's" = Establish / Educate / Enforce**

Conclusion / Questions

- ***Let's be careful out there . . .***

- ***Q+A***

  - **Robert D. Brownstone**
    - <www.fenwick.com/attorneys/4.2.1.asp?aid=544>
    - 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 F&W EIM & Privacy Groups**
  - <www.fenwick.com/services/2.23.0.asp?s=1055>
  - <www.fenwick.com/services/2.14.0.asp?s=1045>

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.