

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

28th Annual

Public Sector EEO and Employment Law Conference

August 28, 2009 – San Francisco, CA

Workplace Privacy Policies

Robert D. Brownstone, Esq.*

**Robert D. Brownstone* is the Law & Technology Director at *Fenwick & West LLP*. He advises clients on electronic discovery, information-security, electronic information management and retention/destruction policies and protocols. Mr. Brownstone also collaborates with clients as to computer solutions enabling compliance with legal obligations.

A nationwide advisor, speaker and writer on many law and technology issues, he is frequently quoted in the press as an expert on electronic information. He also teaches Electronic Discovery classes at the University of San Francisco School (USF) of Law and Santa Clara University School of Law.

Mr. Brownstone is a member of: four state bars; the NELI Advisory Board; and the executive committee of the State Bar of California's Law Practice Management and Technology (LPMT) Section.

Before joining Fenwick & West in 2000, Mr. Brownstone had a varied 13-year career as a litigator, law school administrator, law school teacher and consultant. He received his J.D. *magna cum laude* from Brooklyn Law School in 1986 and his B.A. from Swarthmore College in 1982.

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.

© 2009 Fenwick & West LLP

FENWICK & WEST LLP

SILICON VALLEY • SAN FRANCISCO • SEATTLE • BOISE



Robert D. Brownstone

Law & Technology Director

www.fenwick.com/attorneys/4.2.1.asp?aid=544

Phone: 650.335.7912

Fax: 650.938.5200

E-mail: rbrownstone@fenwick.com

Emphases:

Records Retention/Destruction

Electronic Discovery

Electronic Information Management

Compliance

Privacy and Information Security

Representative Clients:

Capcom Entertainment, Inc.

Daimler Chrysler Corporation

Equinix, Inc.

Interwoven

Omidyar Network

Opware Inc.

Port of Oakland

Proofpoint, Inc.

Xilinx, Inc.

Robert D. Brownstone advises clients on electronic discovery, on electronic information management and on retention/destruction policies and protocols. He also collaborates with clients on computer solutions enabling compliance with legal duties www.fenwick.com/services/2.23.0.asp?s=1055.

A nationwide speaker and writer on many law and technology issues www.fenwick.com/attorneys/4.2.1.asp?aid=544#publications, Mr. Brownstone is frequently quoted in the press as an expert on electronic information www.fenwick.com/attorneys/4.2.1.asp?aid=544#Featured. He also teaches Electronic Discovery classes at the University of San Francisco School (USF) of Law and Santa Clara University School of Law.

Mr. Brownstone is a member of: four state bars (including California and New York); the Information Systems Auditing and Control Association (ISACA) and the Association of Records Managers and Administrators (ARMA). Mr. Brownstone is also the Vice-Chair-Elect of the executive committee of the State Bar of California's Law Practice Management and Technology (LPMT) Section.

In 2007, he was named to the National Employment Law Institute (NELI) Advisory Board. In 2006, Mr. Brownstone was named a Northern California Super Lawyer and featured in a cover story of ABA's *Law Practice* Magazine. www.fenwick.com/pressroom/5.1.1.asp?mid=329&loc=FN.

Before joining Fenwick & West in 2000, he had a varied 13-year career as a litigator, law school administrator, law school teacher and consultant.

From 1995 to 2000, Mr. Brownstone was the Moot Court Program Coordinator at the USF School of Law. During the 1997-98 school year, he also acted as Associate Dean for Academic Affairs and Director of Legal Research & Writing at JFKU School of Law in Walnut Creek, California. From 1992 to 2000, Mr. Brownstone taught Legal Research Writing & Analysis at USF Law.

Between 1990 and 1995, Mr. Brownstone had key roles in some publicized cases. From 1986 to 1990, when Mr. Brownstone practiced in New York, he was on plaintiffs' counsel's team in the civil suit against Claus von Bulow and on Lowell Milken's defense team in multiple Drexel Burnham Lambert matters.

In 1986, Mr. Brownstone received his J.D., *magna cum laude*, from Brooklyn Law School, where he was a Notes Editor and a published author on the *Brooklyn Law Review*. In 1982, Mr. Brownstone received his B.A. in English literature and political science from Swarthmore College.

FENWICK & WEST LLP

SILICON VALLEY • SAN FRANCISCO • SEATTLE • BOISE

Workplace Privacy Policies Materials – TABLE OF CONTENTS

PAGE

PAPER

TABLE OF CONTENTS	i
Body of Paper	1

APPENDICES

App. A – SLIDES	A-1
App. B – “E-MAIL’S NINE LIVES”	B-1
App. C – SAMPLE SUMMARY MEMO RE: TECHNOLOGY ACCEPTABLE USE (AND LACK-OF-EMPLOYEE-PRIVACY) POLICY	C-1
App. D – SAMPLES – GENERIC POLICIES	D-1
SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 1	D-1
SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 2	D-6
SAMPLE ELECTRONIC MAIL POLICY	D-10
SAMPLE ACKNOWLEDGMENT OF RECEIPT	D-14
SAMPLE BLOGGING POLICY	D-15
SAMPLE FCRA DISCLOSURE FOR ADVERSE ACTION BASED ON NON-FACT ACT INVESTIGATIONS	D-17
App. E – BIBLIOGRAPHY # 1 – ELEC. INFO. MGMT. (EIM) RESOURCES	E-1
App. F – BIBLIOGRAPHY # 2 – COMPLIANCE RESOURCES (<i>some</i>) – R. Brownstone and Kevin Moore (Fenwick & West LLP)	F-1
App. G – BIBLIOGRAPHY # 3 – COMPUTER TECHNOLOGY TERMINOLOGY – Online Glossaries Links List.....	G-1
App. H – BIBLIOGRAPHY # 4 – DETROIT TEXT-MESSAGING SCANDAL – Additional Articles.....	H-1

**PAPER TABLE OF CONTENTS
(Continued)**

	Page
I. INTRODUCTION – THE MODERN LANDSCAPE	1
A. Physical Conduct PLUS Digital Activity.....	1
B. Strange Things People Memorialize – Overview of Liability Risks	4
1. Employees’ Damaging Emails.....	4
2. Employees’ Damaging Internet Use and Postings	7
a. Internet Activity.....	7
b. Posts on Chatrooms, Blogs, Wikis, Social Networking Sites, Twitter, etc	8
(i) Company Confidential and Trade Secret Information	10
(ii) Harassment.....	12
(iii) Discrimination	13
(iv) Concerted Activity	13
c. Damaging Metadata and Embedded Data	14
3. Prospective Employees’ (Applicants’) Internet Activity	16
II. MONITORING OF EMPLOYEES’ ELECTRONIC ACTIVITIES	16
A. Introduction	16
B. Legality – Some Justifications and Some Countervailing Concerns	17
1. Federal Electronic Communications Privacy Act (Wiretap And Stored Communications Act)	17
a. Wiretap Act as Applied to E-Mails in Transit.....	19
(i) Majority View – Interception Must be Contemporaneous with Transmission.....	19
(ii) Newer Minority View – Interception need NOT be Contemporaneous with Transmission.....	20
b. Stored Communications Act as Shield and Sword	22
(i) Shield: Employer Access to Stored E-mails, “Private” Web-Based E-mail Systems, Pagers and Employee Web Sites.....	22
(ii) Sword: Affirmative Claim Based on Snooping by Former Employee.....	27
2. State Analogues to the ECPA.....	29

**PAPER TABLE OF CONTENTS
(Continued)**

	Page
3. Computer Fraud and Abuse Act (“CFAA”).....	30
4. Countervailing Concern # 1 – Protected Union Activity Under the National Labor Relations Act, et al. (“NLRA”)	38
5. Countervailing Concern # 2 – Avoiding Invasion of Privacy Claims	41
III. INVESTIGATIONS AND BACKGROUND CHECKS.....	44
A. Credit Report Information Under FCRA/FACTA and State-Analogues	44
1. FACT Act Excludes Workplace Investigations From FCRA Requirements.....	45
2. Non-FACT Act Investigations (Including Background Checks) Must Comply With FCRA Requirements	45
3. Outside Investigations Must Comply with State Regulatory Schemes Such as California’s ICRAA	46
B. Legality and Advisability of Following the Internet Trail	47
IV. SEARCHING, SURVEILLING AND TRACKING PHYSICAL CONDUCT AND LOCATIONS	49
A. Workplace & Personal Searches.....	49
1. Workplace Searches.....	49
2. Personal Searches.....	50
B. Video Surveillance	51
C. GPS Tracking – including RFID and GPS.....	53
D. “Off-Duty” Activities.....	56
1. Competitive Business Activities	56
2. Substance Use	57
3. Dating and Intimate Relationships.....	59
4. Arrests and Convictions	61
5. Miscellaneous Web Activities.....	62
V. IMPLEMENTING LEGALLY-COMPLIANT AND DEFENSIBLE POLICIES	64
A. Introduction to Compliance.....	64
1. The Three E’s – Establish, then Educate, then Enforce.....	64
2. Eliminating Employee Privacy Expectations – Notice, Reasonableness, etc	65

**PAPER TABLE OF CONTENTS
(Continued)**

	Page
B. Some Key Privacy-Related Policies.....	68
1. Policies Eliminating Employee Privacy Expectations.....	68
a. Computer Systems and Hardware Policies.....	68
b. Inspection/Litigation Provisions	73
c. International Caveat.....	74
2. Special Issues Often Ignored: Voicemails/IM's/PDA's.....	74
3. Prohibitions/Restrictions on Blogging, Posting, Social- Networking, Twittering and the Like	75
a. What Position Should My Organization Take With Respect To Blogs, Social-Networking Sites and the Like?.....	75
b. What Options Does My Company Have For Telling Employees Its Position On Web Postings?.....	76
(i) Rely on Existing Policies.....	76
(ii) Revise Existing Policies to Reference Blogs	77
(iii) Supplement Existing Policies with a Blog Policy	78
(a) Additional Documentation.....	79
(b) Supplement Training Materials	79
C. Risks of Strict Policies.....	80
1. Creation of Duty to Act?	80
2. Prohibit Innocent Surfing?	81
D. Periodic Training	82
1. E-mail “Netiquette” (Writing For Multiple Audiences)	82
2. Attorney-Client Privilege.....	83
E. INFORMATION-SECURITY COMPLIANCE CONSIDERATIONS	83
1. IT Compliance Frameworks	83
2. Metadata-Handling and Redaction Protocols	85

I. INTRODUCTION – THE MODERN LANDSCAPE¹

A. Physical Conduct PLUS Digital Activity

Harassing or other discriminatory actions, other conduct leading to liability to third-parties, forbidden fraternizing, criminal activity, “frolic and detour” or other slacking have been traditional concerns for employers. So has loss of information sensitive to the employer, employees, related organizations and even adversarial entities.

Workplaces have become increasingly digitized, as a ramification of electronic information’s predominance in all aspects of modern life.² Much less than 1% of business information is being created exclusively in paper form.³ Thus, upwards of 99% of the world’s information initially existed as a data file.⁴ Though estimates vary, in most companies, 70% to 95% of information ends up being stored only in electronic form and thus never printed to paper.⁵ Seven trillion e-mails are sent annually; 60-200 daily to the average employee.⁶ In short, “[g]one are the days when all that “business technology” meant was a telephone, an adding machine and carbon paper.”⁷

¹ The author thanks his current colleagues Allen Kato, Ilana Rubel, Vic Schachter and Mary Wang – as well as his former colleagues John Fox, Juleen Konkell, Patrick Sherman and Shawna Swanson – for their contributions of prior content on which parts of this white paper are based.

² See, e.g., Maag, Christopher, *Tracking Thieves, or Teens; Technology, the Stealthy Tattletale*, N.Y. Times (Oct. 26, 2007).

³ See Peter Lyman & Hal R. Varian, *How Much Information? 2003* (Oct. 30, 2003), <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf> (reporting only 0.01% of new information is stored in paper form); cf. Peter Lyman & Hal R. Varian, *How Much Information? 2000* (Nov. 10, 2000), <<http://www2.sims.berkeley.edu/research/projects/how-much-info/how-much-info.pdf>> (reporting printed documents comprise only 0.003% of total documents). See generally Robert D. Brownstone, *Preserve or Perish; Destroy or Drown – eDiscovery Morphs Into Electronic Information Management (EIM)*, 8 N.C. J.L. & Tech., No. 1, at 1 (Fall 2006) (hereafter “Brownstone N.C. JOLT”) <http://jolt.unc.edu/sites/default/files/8_nc_jl_tech_1.pdf>; Collaborative Navigation of the Stormy eDiscovery Seas, 10 RICH. J.L. & TECH. 53 (2004) (hereafter “Brownstone Richmond JOLT”) <<http://law.richmond.edu/jolt/v10i5/article53.pdf>>.

⁴ *Id.*

⁵ “[Seventy percent] of corporate records may be stored in electronic format, and [thirty percent] of electronic information is never printed to paper.” See *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production 4* (July 2005), <http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf#page=14>; cf. William A. Fenwick, *Electronic Records: Opportunity for Increased Efficiency*, Applied Discovery Orange Pages Electronic Discovery Newsletter 4 (June 2003) (higher estimate of 90-95%) <www.lexisnexis.com/applieddiscovery/lawlibrary/newsletter/TheOrangePages_Jun03_.pdf>.

⁶ David Friedman, *Tips For More Effective Email Communication*, Connections (Sep. 1, 2005) <<http://www.connectionsmagazine.com/articles/5/072.html>>.

⁷ Sherrie Travis, *Mitigating Liability From Employee Use of Technology*, Corp. Counselor (July 19, 2007) <www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1184869650782> (“Travis”).

With the advent of Web 2.0 and User-Generated content – blogs, wikis, social networking sites and Twitter – there are heightened concerns. In the era of data proliferation, employers have a legitimate interest in protecting themselves. Employees have access to, and are the gatekeepers of, trade secrets and other sensitive and confidential information. A single negligent⁸ or malicious employee can cause truly irreparable harm.

One constituency at risk for data leakage is the group of employees. In the past six months, two highly publicized incidents ostensibly involved the loss of personally identifiable information (“PII”) as to 97,000⁹ and 29,000¹⁰ co-workers, respectively. In the latter situation, the theft occurred while the data was in the possession of the employees’ labor union.^{9.5}

Employers face an increasingly challenging environment with new and sometimes conflicting responsibilities to employees. Millions of employees’ electronic activities are under “continuous surveillance” as to content, length, attachments, time spent, and

⁸ See, e.g., Dan Slater, *Lawyer’s Email Slip-up Leads to Zyprexa Leak*, Wall St. J. Law Blog (Feb. 2, 2008) <<http://blogs.wsj.com/law/2008/02/05/report-lawyers-email-slip-up-leads-to-zyprexa-leak/>>.

⁹ 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>>. See 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”) <www.fenwick.com/publications/6.5.4.asp?mid=44&WT.mc_id=EB_031209>; BNA, *Worker Files Class Action Against Starbucks In Laptop Breach of 97,000 Employees’ Data*, 8 PVLR 336, Privacy & Security Law Report (Mar. 2, 2009), (noting irony that “A December 2008 Ponemon Institute study found that consumers ranked Starbucks as the most trusted company in the food service industry for protecting their privacy”) <http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=11636455&vname=pvlrnotallissues&fn=11636455&jd=A0B7Z3D6R5&split=0> (subscription required to use URL).

¹⁰ Sandy Kleffman, *Kaiser warns nearly 30,000 employees of data breach*, Contra Costa Times (Feb. 6, 2009) (“‘handful’ of employees have reported identity thefts as a result of stolen information [that] included names, addresses, dates of birth and Social Security numbers”) <http://www.mercurynews.com/ci_11646163?nclick_check=1>.

^{9.5} Sandy Kleffman, *Kaiser: Stolen data was from union offices*, Contra Costa Times (Feb. 27, 2009) (“[I]aw enforcement detectives have determined the information was taken from the offices of [UHW]-West[;] . . . Kaiser has offered to provide one year of free credit monitoring to affected employees.”) <http://www.mercurynews.com/breakingnews/ci_11804740?nclick_check=1>.

keystrokes.¹¹ Next-generation capabilities now include measures such as: biometrics for security, timekeeping and attendance;¹² recording employees' voice-based and data-based conversations;¹³ and virtual call-center software that can monitor workloads and productivity of work-at-home independent contractors.¹⁴

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. While employers, in pursuing legitimate objectives, may make some 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. Taming the three-headed compliance monster is not easy.

¹¹ "41% of US companies with 20,000 or more employees surveyed employ staff to read or otherwise analyze outbound email. Overall, more than one quarter (29%) of US companies surveyed employ such staff." Proofpoint, *Outbound Email and Data Loss Prevention in Today's Enterprise*, 2008 (May 2008), at ii (.pdf p. 4) <<http://www.proofpoint.com/downloads/Proofpoint-Outbound-Email-and-Data-Loss-Prevention-in-Today's-Enterprise-2008.pdf>> ("44% of US companies investigated a suspected email leak of confidential or proprietary;" "26% terminated an employee for violating email policies") See also American Management Association (AMA) and ePolicy Institute, *2005 Electronic Monitoring & Surveillance Survey* <<http://www.amanet.org/press/amanews/ems05.htm>>; Andrea Coombes, *Privacy at Work? Don't Count on It: Employers Are Tracking Email*, Wall St. J. (July 1, 2005) <<http://www.careerjournal.com/myc/killers/20050701-coombes.html>>; Paula Brantner, *Blogging Employees, Beware* (Workplace Fairness June 21, 2005) <http://www.workplacefairness.org/2005_06_01_pblog_archive.php>.

¹² Molly DiBianca, *Workplace Privacy: Biometrics May Be Coming to a Workplace Near You*, (Apr. 20, 2008) ("[u]nlike traditional security measures, like passwords or security badges, biometrics cannot be shared, lost, forgotten, stolen, or recreated") <www.delawareemploymentlawblog.com/2008/04/workplace_privacy_biometrics_m.html?action=print>.

¹³ Renai LeMay, *RIM changes tune on employee calls*, cnet news (Mar. 18, 2009) <http://news.cnet.com/8301-1035_3-10199076-94.html>.

¹⁴ 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>>.

B. Strange Things People Memorialize – Overview of Liability Risks

1. Employees' Damaging Emails¹⁵

Throughout this decade, e-mail messages have become pivotal in litigation. A 2006 study found that 24% of companies had been ordered by courts to produce employee emails and 15% of companies had battled lawsuits stemming from employee emails.¹⁶

Emails are quick, cheap and easy means of communication. They also tend to be more candid, less formal and less thoughtful than other writings.¹⁷ Still, half of U.S. and U.K. companies fail to offer, let alone require, e-mail training for their employees.¹⁸ In any event, e-mail's status as an indispensable business tool has also posed numerous potential threats for employers.

In harassment or discrimination cases, one or two explicit messages can bolster other evidence of hostile environment or discrimination.¹⁹ In the highly-publicized case of *Zubulake v. UBS Warburg*,²⁰ Laura Zubulake, a former Wall Street executive, sued UBS alleging that the bank discriminated against her because she was a woman and then retaliated against her when she complained about her treatment. During the course of litigation, Plaintiff produced over 450 pages of relevant emails, including a "smoking gun" email written by defendants suggesting that Zubulake be fired "ASAP" after her Equal Employment Opportunity Commission (EEOC) charge was filed, in part so she would be ineligible for year-end bonuses.

The jury awarded Zubulake over \$29 million in total damages. Similarly, a Chevron subsidiary was apparently induced to settle a sexual harassment claim in 1995 for \$2.2 million, based on unearthed evidence including e-mailed jokes such as "25 reasons why

¹⁵ The most current version is: "Would you like it in the press? . . . Would you like to see it on a competitor's desk? . . . Would you like it in the government's hand? . . . Would you like to read it on the witness stand? If the content will get you slammed, then . . . DO NOT SEND IT, SAM I AM." © Fenwick & West LLP; Mark Ostrau & Robert Brownstone <www.fenwick.com/services/2.23.0.asp?s=1055>. Cf. Sharon D. Nelson, Esq. and John W. Simek, *D'OH!!!! The Dumb Things Lawyers Do with E-Mail*, Sensei Enters. (2006) <<http://www.senseient.com/e-mail%20mistakes.asp>>.

¹⁶ See American Management Association and ePolicy Institute, *2006 Workplace E-Mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators*, available at <http://www.amanet.org/press/amanews/2006/blogs_2006.htm/>.

¹⁷ Brownstone N.C. JOLT, *supra* note 3, at 3-6.

¹⁸ Proofpoint, *Outbound Email and Data Loss Prevention in Today's Enterprise, 2008* (May 2008), at 14 <<http://www.proofpoint.com/downloads/Proofpoint-Outbound-Email-and-Data-Loss-Prevention-in-Today's-Enterprise-2008.pdf>>.

¹⁹ Brownstone N.C. JOLT, *supra* note 3, at 5-6.

²⁰ *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake I*") <<http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF>>.

having beer is better than having women.”²¹ Likewise, e-mails between former Boeing CFO Michael Sears and the daughter of Air Force procurement officer Darleen Druyun led to Sears’ hiring Druyun while she could still influence Air Force buying decisions – and to their both being fired in November 2003.²²

In today’s world, one regularly learns of pivotal “smoking guns” e-mails or other types of digital gaffes in:

- business,²³
- national politics,²⁴ and

²¹ Hundley, Kris, *Medical industry taught legal perils of saying, e-mailing too much*, St. Petersburg Times (Feb. 6, 2009) <<http://www.tampabay.com/news/business/article973694.ece>>. See also Ann Carns, *Prying Times: Those Bawdy E-Mails Were Good for a Laugh—Until the Ax Fell*, Wall St. J., Feb. 4, 2000, at A8.

²² Dan Richman, “Boeing E-mail Bites Back”, “E-mails sent at work anything but private,” Seattle Post Intelligencer (Mar. 9, 2005) <http://seattlepi.nwsourc.com/business/215147_email09.html>.

²³ See, e.g., Peter B. Matuszak, *Los Angeles' Lawsuit Alleges Massive Wall Street Bond Conspiracy*, L.A./S.F. Daily J. (July 24, 2008), available at <<http://www.carealestatejournal.com/newswire/index.cfm?sid=&tkn=&eid=895686&evid=1>>; Pamela A. MacLean, *Plaintiffs Score With E-Mail Evidence in Multidistrict Price-Fixing Case*, Nat'l L.J. (July 7, 2008) <<http://www.law.com/jsp/article.jsp?id=1202422773207>>; Justin Sheck, *Options Morass Deepens at Sonsini Firm*, Recorder (Mar. 29, 2007) <<http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1175072636313>>; Peter Lattman, *Wilson Sonsini & the “Time Machine” Email*, WSJ Law Blog (Mar. 29, 2007) <<http://blogs.wsj.com/law/2007/03/29/wilson-sonsini-the-time-machine-email/>>. Cf. Abate, Tom, *Video raises concern about firms' H-1B abuses; 2 lawmakers urge labor secretary to probe 'blatant disregard for American workers'*, S.F. Chronicle (June 22, 2007) <<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2007/06/22/BUGOOQJHN41.DTL&type=printable>>.

- local politics.²⁵

²⁴ See, e.g., Anick Jesdanun, *White House e-mail recovery not trivial*, AP (Apr. 13, 2007); John D. McKinnon, *Congress Follows E-mail Trail*, Wall St. J. (Apr. 10, 2007) <http://online.wsj.com/public/article/SB117615846511864432-61WsY8Df7s6_Oa_SaheNaLuEug4_20080408.html#printMode> Michael Abramowitz & Dan Eggen, *White House E-Mail Lost in Private Accounts* Wash. Post (Apr. 12, 2007) <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/11/AR2007041102167_pf.html>; Washington Post, *E-Mails Offered in Qwest Trial* (Apr. 4, 2007) <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/03/AR2007040301845_pf.html>; Peter Lattman, *From: Law Blog, To: Reader, Subject: U.S. Attorney Mess*, Wall St. J. (Mar. 13, 2007) <<http://blogs.wsj.com/law/2007/03/13/from-law-blog-to-law-blog-reader-subject-us-attorney-mess/>> (linking to 25 pages of e-mails at <http://judiciary.house.gov/media/pdfs/DOJdocsPt1070313.pdf>); Sierra Club, *This Species Is in Danger A-OK!; A Bush bureaucrat hurries critters to the grave* (Mar./Apr. 2007) (e-mails and other documents reflecting “deputy assistant secretary in the Department of the Interior . . . repeatedly disregarded the recommendations of career scientists, even changing their findings”) <<http://www.sierraclub.org/utilities/printpage.asp?REF=/sierra/200703/decoder.asp>>; US DOJ IG, *Review of FBI’s Initial Response to Rep. Mark Foley’s E-mails to a Former Page* (Jan. 22, 2007) <<http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/foley/fbioig12207rpt.pdf>>; Dana Bash, *Congressman quits after messages to teens found*, CNN.com (Sep. 29, 2006) <<http://FoleyIM.notlong.com>>; Complaint, *In re Mercury Interactive Corp. Derivative Litig.*, No. 1:05-cv-50710 (Cal. Super. Santa Clara 9/22/06) (“I betcha that [she] will overrule these types of things . . . and we will use her magic backdating ink. Let’s see what happens!”) <http://online.wsj.com/public/resources/documents/WSJ_Mercury022007.pdf>; Mark Boslet and Mark Maremont, *Emails Reveal Backdating Scheme*, Wall St. J. (Feb. 20, 2007) (“Mercury Complaint Claims Wide Efforts Among Executives”) <http://online.wsj.com/article_print/SB117176028286012442.html>; Indictment, *U.S. v. O’Keefe and Agrawal*, No. 1:06-cr-00249-PLF (D.D.C. Aug. 18, 2006) (career State Department official accused of accepting bribes – including free trips – in exchange for trying to expedite H-1 visa application process for employees of CEO of NYC-based jeweler) <https://ecf.dcd.uscourts.gov/cgi-bin/show_case_doc?2,122129,,,,,9,1>; *U.S. Visa Official; Indicted for Bribery* (Findlaw Breaking Documents Aug. 25, 2006) <<http://news.findlaw.com/hdocs/docs/dos/usokeefe81806ind.html>>; Snopes.com E-mail Exchanges, *Ketchup Trousers* (“[I]aw firm secretary sends caustic reply to senior associate’s e-mail request for a[n \$8] cleaning bill reimbursement”) <<http://www.snopes.com/embarrass/email/ketchup.asp>>.

²⁵ See, e.g., Janine Zúñiga, *A political soap opera plays out via e-mail*, S.D. Union-Tribune (Oct. 31, 2008) (including “E-mail do’s and don’ts”) <<http://www.copleynews.com/news/politics/20081031-9999-1m31email.html>>; Tresa Baldas, *Detroit’s former mayor is out of jail, but not out of legal problems*, Nat’l L.J. (Feb. 4, 2009) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202427983943>>. For many other articles on the Detroit text-messaging scandal, see Appendix H to this paper.

2. Employees' Damaging Internet Use and Postings

In addition to e-mail, Internet content and postings (on blogs, wikis, social networking sites, Twitter, etc.) create written business records that are the electronic equivalent of DNA evidence.²⁶

a. Internet Activity

The Internet has emerged as the "modern equivalent of a telephone or a daily newspaper, providing a combination of communication and information that most employees use as frequently in their personal lives as for their work."²⁷ Employee Web-surfing, however, can entail visiting pornographic websites,²⁸ not only cutting into productivity but also potentially creating a hostile work environment. Furthermore, Web-surfing can cause serious security breaches for companies.

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.²⁹ In 2006, the Oregon Department of Revenue had to contact some 2,300 taxpayers to notify them that their names, addresses or Social Security numbers may have been stolen by a Trojan horse program downloaded accidentally by a former employee who had been surfing pornographic sites while at work.³⁰

²⁶ Nancy Flynn, *Many Companies Monitoring, Recording, Videotaping – and Firing – Employees* (ePolicy Inst. 5/18/05) <<http://www.amanet.org/press/amanews/ems05.htm>>.

²⁷ *Dep't of Educ. v. Choudhri*, No. 722/06, at 12 (N.Y.C. Off. of Admin. Trials & Hearings Mar. 9, 2006) <<http://files.findlaw.com/news.findlaw.com/hdocs/docs/nyc/doechoudri30906opn.pdf>>.

²⁸ See *eDisaster Stories* <<http://web.archive.org/web/20070407143344/http://www.epolicyinstitute.com/disaster/stories.html>> (as to firefighters in Columbus, Ohio, "a routine scan of on-the-job web surfing revealed that the division headquarters' staff members were visiting as many as 8000 pornographic sites a day"); see also *Beware Cyberslackers, Spammers* <<http://web.archive.org/web/20071020224507/http://www.epolicyinstitute.com/ipolicies/index.html>> (noting "90% of workers admit to recreational surfing on company time, accounting for nearly one third of their online activity;" and "[c]yberslackers' favorite sites [were] general news 29.1%; investment 22.5%; [and] pornography 9.7%").

²⁹ 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>>.

³⁰ Todd Weiss, *Trojan Horse Captured Data On 2,300 Oregon Taxpayers From Infected Gov' PC*, *Computerworld* (June 15, 2006) <www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001222>.

Other lurking potential dangers include phishing and/or whaling schemes as well as e-mail messages containing malware and/or links to malicious websites.³¹

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

The various 21st century platforms mentioned in Section I above raise many risk-management legal issues.

In addition to chatrooms, online bulletin boards and Web surfing, there is now the “blog,” also known as “weblog.” A blog is an often updated Web-based diary that, until the advent of social-networking, had become “the hottest phenomenon on the Internet.”³² Built on a conversational model, paradoxically, a blog is often not only intimate, but also encourages public discussion.³³

Along with the proliferation of blogs, companies find themselves faced with many new for a for employee conduct that pose legal risk for employers. One ramification of employee blogs can be “doocing”—namely, the firing of an employee for his or her posting of negative comments about the company on a personal blog.³⁴ The most commonly cited objection regarding terminations based on personal blogging is the lack of notice that the offending conduct was problematic.³⁵

The ramifications for employers from the content of employee blogs or from leaks to non-employee blogs or sites include intentional or unintentional disclosure of confidential

³¹ See, e.g., Niraj Chokshi, *O'Melveny's Name Slapped Onto Web Scam*, Legal Pad (Apr. 14, 2008) (fake grand jury subpoena) <http://legalpad.typepad.com/my_weblog/2008/04/omelvenys-name.html>; Deborah Gage, “Computer worm spreads holiday infection,” SF Chronicle (Dec. 29, 2007) (“Storm Worm”) <<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2008/02/15/BU47V0VOH.DTL&type=printable>>.

³² Walter S. Mossberg, *Taking the Mystery Out of Blog Creation*, Wall St. J. (June 15, 2005), at D4 <<http://Blog-Article-WSJ-6-15-05.notlong.com>>.

³³ *Id.*; Lee Rainie, *The State of Blogging*, Pew Internet & Am. Life Project (Jan. 1, 2005) <http://www.pewinternet.org/pdfs/PIP_blogging_data.pdf>; Yuki Noguchi, *Cyber-Catharsis: Bloggers Use Web Sites as Therapy*, Wash. Post (Oct. 12, 2005), at A1 <www.washingtonpost.com/wp-dyn/content/article/2005/10/11/AR2005101101781_pf.html>.

³⁴ See Heather Armstrong, *About This Site* <<http://www.dooce.com>> (coining the phrase “dooce”); <www.pcmag.com/encyclopedia_term/0,2542,t=dooce&i=41700,00.asp>; see also Joyce Cutler, *Beware Pitfalls Created By Employee Blogging*, Pike & Fischer DDEE (May 16, 2005) (citing *Konop v. Hawaiian Airlines Inc.*, 302 F.3d 868 (9th Cir. 2002) <<http://Konop11-9thCir-8-23-02.notlong.com>>); Stephanie Armour, *Warning: Your Clever Little Blog Could Get You Fired*, USA Today (June 14, 2005) <http://www.usatoday.com/money/workplace/2005-06-14-worker-blogs-usat_x.htm>.

³⁵ In an apparent backlash to the way some companies have treated employees because of their blogs, organizations such as the Electronic Frontier Foundation (EFF) have created “Bloggers’ Rights” guides. See EFF, *EFF: Fighting for Bloggers’ Rights* <<http://w2.eff.org/bloggers/>> (last visited Nov. 2, 2008).

information,³⁶ and vicarious liability for content claimed to be harassing or otherwise actionable.³⁷ As to intentional disclosures, one troublesome scenario can entail an insider's pseudonymous, *favorable* postings on a public site.³⁸ This practice is called "sock-puppeting."³⁹ As to harassment, even non-sponsored bulletin boards can be so closely related to the environment and/or so beneficial that they are deemed part of the workplace.

Companies are constantly responding to a changing technological environment. From handwriting to typewriters, to word processors, to computers, each step has facilitated quicker and more widespread communication.⁴⁰ Until fairly recently, companies had dealt with legal issues surrounding a certain limited set of eCommunications – such as email and IM. Now, there are many more types of forums on which to focus. Specific concerns include protecting employer trade secret information and preventing harassment.

Blogs – as well as wikis, employees' respective individual home pages on social networking sites, ill-advised tweets on Twitter⁴¹ and postings in chatrooms (including

³⁶ See, e.g., Ben Arnoldy, *Close of Wikileaks website raises free speech concerns*, Christian Science Monitor (Dec. 22, 2008) ("US judge's move to close the dissident site...showed the limits of enforcing national laws in cyberspace") <<http://Wikileaks-CSM-2-22-08.notlong.cm>>. Cf. Ed Frauenheim, *Starbucks Employees Carve Out Own Space*, Workforce Management (Oct. 2, 2007) <<http://www.workforce.com/section/10/feature/25/20/77/252079.html>>.

³⁷ Tresa Baldas, *Work Blogs Take Off, and So Do the Suits*, Nat'l L.J. (Sep. 18, 2008) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202424595821>>.

³⁸ See, e.g., Andrew Martin, *Whole Foods Executive Used Alias*, N.Y. Times (July 12, 2007) <<http://nytimes.com/2007/07/12/business/12foods.html?pagewanted=printable>>.

³⁹ See, e.g., Brad Stone and Matt Richtel, *The Hand That Controls the Sock Puppet Could Get Slapped*, N.Y. Times (July 16, 2007) ("on the Internet nobody knows you're a dog – or the chief executive;" distinguishing Whole Food's CEO's sock-puppeting from more formalized, byline-containing blogs generated by Sun Microsystems, Marriott International and Pitney-Bowes) <<http://www.nytimes.com/2007/07/16/technology/16blog.html?pagewanted=print>>.

⁴⁰ David Kesmodel, *Whole Foods Bars Executives From Web Forums*, Wall St. J. (11/7/07)

⁴¹ To learn more about tweeting on Twitter and/or engaging in online social networking, see 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/onlineexclusives/twitter.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) <<http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202429165569>>; Pogue, David, *The Twitter Experiment*, N.Y. Times (Jan. 29, 2009) <<http://www.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) <www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202426916023>.

perhaps, via sock-puppetry⁴²) – likely comprise the next step: the same law in new contexts. Throughout the ensuing (sub-)sections of this Paper (and when reviewing the samples attached as Appendix D), please interpret each reference to “blog” to encompass all of the many ways any given individual can become a publisher in our modern world.

(i) Company Confidential and Trade Secret Information

Trade secret law and employee invention-assignment and proprietary-information agreements prohibit the unauthorized use or disclosure of an employer’s trade secrets and confidential information – whether or not the information is written in a book, used to create an invention, or posted to the Internet through a blog. Notwithstanding the many steps employers take to protect the secrecy of their information (and that of their customers and partners), blogs present a particular threat. Blogs have the capability to undermine the secrecy of confidential information due to the informal nature of the communication and the broad access the Internet provides to blog postings.

One obvious threat is the possibility that an employee will intentionally disclose company information. For example, a disgruntled former employee might disclose his former company’s confidential or trade secret information (such as an internal list of bugs in its product or a failed attempt to create a new feature in the product) as revenge for what the employee perceived as an unfair termination. Furthermore, employees may disclose such information to gain popularity or make their blogs more interesting.

A famous “blogger” case may have arisen from such a disclosure. In *Apple Computer, Inc. v. Does, et al.*,⁴³ Apple sued unidentified individuals and entities for the alleged disclosure, via blogs, of Apple’s confidential information about “a FireWire audio interface for Garage Band, codenamed ‘Asteroid’ or ‘Q7.’” Websites including Apple Insider and PowerPage published this information. Apple subpoenaed Nfox, the email service provider for PowerPage, to obtain emails that might identify the source of the information. Jason O’Grady and two others (“O’Grady”), who self-identified as journalists but are more appropriately called “bloggers,” moved for a protective order claiming a privilege from disclosing confidential sources and other protections.

Ultimately, the appellate court ruled that O’Grady’s alleged privilege did justify a protective order.⁴⁴ Thus, the employer could not determine the source(s) of the leak. Note that, in the federal courts, pending Congressional legislation may also provide protection for anonymous sources. In the Spring of 2007, the House Judiciary Committee approved the

⁴² See footnotes 39-40 and accompanying text supra.

⁴³ *O’Grady v. Super. Ct.*, 44 Cal. Rptr. 3d 72 (Cal. App. 6 Dist. 2006) (deciding, unanimously, to strike down subpoenas to Internet “news” sites seeking source of trade secret information leaked to bloggers), *rev’g Apple Computer, Inc. v. Does*, No. 1-04-CV-032178, 2005 WL 578641 (Cal. Super. Mar. 11, 2005) (denying motion for protective order where anonymous, fame-seeking employees had leaked confidential product information to bloggers). See also case archive at <[http://www.eff.org/Censorship/Apple v Does/](http://www.eff.org/Censorship/Apple_v_Does/)>.

⁴⁴ *O’Grady v. Super. Ct.*, 44 Cal. Rptr. 3d 72 (Cal. App. 6 Dist. 2006).

"Free Flow of Information Act of 2007,"⁴⁵ whose companion bill, S. 2035, stalled in the Senate between October 2007 and July 2008.⁴⁶

Disclosures, however, need not be so obvious or intentional to result in damage to a company. For instance, an employee may discuss her work on her blog without identifying her employer but nevertheless disclose confidential information. Or, an employee may post what he believes to be a funny or ironic fact (or photo) that the employer considers to be sensitive or even defamatory.

For example, in October 2003, Microsoft ended Michael Hanscom's temporary stint with Xerox at the Microsoft campus after Mr. Hanscom took a photo on the campus and posted it to his blog.⁴⁷ Mr. Hanscom, a longtime Mac fan, found the presence of stacked boxes of Apple Macintosh G5's on Microsoft's loading dock too funny to pass up. He took a picture of the boxes and posted it to his blog with the following caption: "Even Microsoft wants G5s." Microsoft indicated the posting was a security violation, in that contractors were required to sign confidentiality agreements, and thus let him go.

In the government setting, a similar fate befell a CIA software contractor, who posted an inordinate amount of information "in her blog, which, in turn, was hosted on Interlink, the intelligence community's classified intranet."⁴⁸ "Writing as Covert Communications, CC for short, she opined in her online journal on such national security conundrums as stagflation, the war of ideas in the Middle East and – in her most popular post – bad food in the CIA cafeteria."⁴⁹ "On July 13[, 2006], after she posted her views on torture and the Geneva Conventions, her blog was taken down and her security badge was revoked. [S]he was terminated by her employer . . . which was helping the CIA test software."⁵⁰

Under the prior examples, the employees would bear liability for the unauthorized use or disclosure of confidential information; however, employees can also create liability for their employers by disclosing the confidential or trade secret information of the employer's customers or business partners – and, in the public sector, of the public and/or the pertinent

⁴⁵ See <<http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.02102>>. For a videotape of the pertinent Judiciary Committee hearing, go to <http://judiciary.house.gov/hearings/June2007/hear_061407.html>. See also Scott Gant, *We're All Journalists Now: The Transformation of the Press and Reshaping of the Law in the Internet Age*, (Free Press June 12, 2007), for sale at <<http://www.amazon.com/Were-All-Journalists-Now-Transformation/dp/0743299264>> and reviewed in Debra Bruno, *Bloggers' Rights a New Book Argues That We're All 'Citizen Journalists'*, June 2007 Am. Law. 85.

⁴⁶ See <<http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.02035>>.

⁴⁷ See Jon Bonné, *Blogger dismissed from Microsoft; Copy shop worker loses position after posting Mac photo* (October 30, 2003) <<http://www.msnbc.msn.com/id/3341689/>>.

⁴⁸ Dana Priest, *Top-Secret World Loses Blogger; CIA Contractor is Fired When Internal Post Crosses the Line*, Wash. Post (July 21, 2006) <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/20/AR2006072001816_pf.html>.

⁴⁹ *Id.*

⁵⁰ *Id.*

agency itself. Thus, when analyzing the content of employees' blogs, it is important for companies to focus not only on protection of their own proprietary interests but those of third parties as well.

(ii) Harassment

In one of the first decisions involving sexual harassment in cyberspace, in 2000 the New Jersey Supreme Court determined that an employer may be liable for its employees' electronic posts to a bulletin board. In *Blakey v. Continental Airlines*,⁵¹ Blakey sued Continental Airlines and several of its male pilots for, among other claims, defamation and sexual harassment based upon a hostile workplace environment. Blakey was the airline's first female captain to fly an Airbus aircraft seating 250 passengers. She alleged that, after her complaints had come to the fore, some of the airline's male pilots published defamatory and harassing electronic messages online – on a computer bulletin board called the Crew Members Forum.

The Forum was accessible to all Continental pilots and crew members through an Internet Service Provider (ISP), CompuServe. While Continental Airlines required that pilots and crew access CompuServe to learn their flight schedules and assignments, the Crew Members Forum was voluntarily accessed by crew members to exchange ideas and information, at their own cost. Blakey and at least one other co-Plaintiff/ female-pilot claimed that the offensive postings had constituted sexual harassment and discrimination. Those postings included "If the porn bothers you, don't look," and "Now don't start your feminazi routine with me."

The New Jersey Supreme Court ruled that sexual harassment and other forms of workplace discrimination can give rise to liability when it occurs in cyberspace, as well as in a physical space that the company controls.⁵² Recognizing that an electronic bulletin board may not have a physical location within a terminal or an aircraft,⁵³ the court ruled that it nevertheless may be so closely related to a workplace environment, and so beneficial to the functioning of the airline, that the Forum was to be regarded as part of the workplace in determining whether harassment occurred. While holding there was no strict obligation on the part of the airline to monitor the bulletin board, the court ruled that the airline was obligated to redress complaints of harassment.

Parallels between posting of a message to a bulletin board and creating and maintaining a blog make *Blakey's* analysis of the sexual harassment claim particularly relevant. Both involve: an electronic message available in cyberspace; and individuals accessing the electronic communications voluntarily. Under such circumstances, according to *Blakey*, the communication is relevant to (and can be the basis for) a hostile work environment claim.

⁵¹ *Blakey v. Continental Airlines*, 164 N.J. 38, 751 A.2d 538 (2000)
<<http://lawlibrary.rutgers.edu/courts/supreme/a-5-99.opn.html>>.

⁵² *Id.*

⁵³ In addition, the court found that personal jurisdiction existed over the defendant pilots since Continental Airlines had its headquarters and main operations in New Jersey, and there were sufficient contacts within that state, notwithstanding that the alleged cyberspace harassment had no particular geographical, territorial presence. *Id.*

The type of blog – personal or corporate – may also factor into the analysis. Under *Blakey*'s "closely related" and/or "beneficial" rationales, a company-sponsored blog will likely be considered a part of the workplace in evaluating whether a post to the blog creates a hostile work environment. In any event, the *Blakey* court ostensibly determined that, at least under New Jersey law, an employer has a duty to investigate reports of sexual harassment – whether involving a personal or a corporate blog.

(iii) Discrimination

An employer's adverse action based on the content of a blog is governed (and limited by) the same anti-discrimination laws and standards applied to other adverse employment actions. An employer may not terminate or discipline the employee based on a protected characteristic. Stated another way, an employer must enforce its policies (including its blog policy, if it has one) without regard to any protected characteristic, including race, sex, age, national origin, disability and sexual orientation.

A former Delta Airlines flight attendant challenged her termination, purportedly for the content of her blog, as unlawful sex discrimination.⁵⁴ Ellen Simonetti filed a claim with the Equal Employment Opportunity Commission against her former employer, Delta Airlines. Ms. Simonetti alleged she was terminated for posting several images on her blog. Among the images was a photograph of Ms. Simonetti posing in her flight attendant uniform in an arguably suggestive pose. Ms. Simonetti claims her termination constituted sex discrimination because Delta Airlines had not disciplined or terminated male colleagues for similar conduct. To date, no decision has been reported on Ms. Simonetti's complaint.

Employers should take a cue from that complaint. Just as with any other type of employee misconduct, employers must take into account their own policies and the law when deciding when and how to discipline employees for blog content. One key to avoiding liability when imposing discipline (and that should also be a regular practice) is to act consistently when addressing conduct by similarly-situated employees.

(iv) Concerted Activity

Section 7 of the National Labor Relations Act ("NLRA") protects employees' rights to engage in "concerted activity for the purpose of . . . mutual aid and protection."⁵⁵ Employers that interfere with these rights may violate Section 8(a)(1) of the NLRA.⁵⁶ These rights are not limited to the union setting; rather, employees enjoy Section 7 rights whether or not they are part of a union labor force.

What does this rule mean for employers?

As to corporate-sponsored blogs, an employer that permits employees to express personal opinions and convey non-business information in such

⁵⁴ Delta employee fired over blog sues airline, AP (Sep. 8, 2005) <<http://www.msnbc.msn.com/id/9259944/>>.

⁵⁵ 29 U.S.C. § 157.

⁵⁶ See 29 U.S.C. § 158(a)(1).

blogs should be cautious about disciplining employees for the content of blogs geared at labor organizing or other arguably protected activity (such as criticizing management, raising safety concerns or comparing compensation).

As to personal blogs, to the extent an employer permits employees to use company equipment⁵⁷ for non-business purposes (for instance, to check a personal email account or surf the Internet), an employer should similarly be cautious about disciplining employees for labor organizing or other arguably protected activity based on the content of the blog or on the employee's use of company resources to update the blog.

c. Damaging Metadata and Embedded Data⁵⁸

Metadata, commonly described as “data about data,” is defined as “information describing the history, tracking, or management of an electronic document.”⁵⁹ File system metadata “describes when a file was created, where it was stored, and what programs the computer uses to help access the file.”⁶⁰ More significantly, an electronic file – especially if disseminated as an e-mail attachment – may contain embedded data, *i.e.*, evidence of prior

⁵⁷ For a thorough discussion of potential NLRA rights of private sector blogging employees who do not use company time or equipment, see Katherine M. Scott, *When is Employee Blogging Protected by Section 7 of the NLRA?* 2006 Duke L. & Tech. Rev. 0017 (2006) <<http://www.law.duke.edu/journals/dltr/articles/pdf/2006DLTR0017.pdf>>.

⁵⁸ George William Herbert, *More PDF Blackout Files*, Slashdot (June 22, 2006) <http://it.slashdot.org/article.pl?no_d2=1&sid=06/06/22/138210> (federal prosecutor filing exposing supposedly redacted names of ballplayers, including Barry Bonds; linking to <www.sfgate.com/c/acrobat/2006/06/22/BALCO_quash_subpoena_sfchronicle.pdf>); see also Dana J. Lesemann, *Copy, Paste and Reveal*, Legal Times (Jan. 30, 2006) <<http://Lesemann-1-30-06.notlong.com>> (U.S. military report as to shooting, in Iraq, of Italian intelligence officer; secret details revealed re: manning of security checkpoints).

⁵⁹ *Williams v. Sprint*, 230 F.R.D. 640 (D. Kan. 2005) (analyzing 12/1/06 version of Fed. R. Civ. P.) <www.ksd.uscourts.gov/opinions/032200JWLDJW-3333.pdf#page=10>. To learn more about metadata, see some of the author's articles and presentations cited/linked in Appendix E as well as Commentary, *Dangers of Document Metadata*, Workshare (2004) <http://www.workshare.com/collateral/misc/Dangers_of_Document_Metadata.pdf> (free registration); David H. Schultz, *Defining Metadata; Counsel's Duty to Preserve and Produce Brought Forefront In Recent Case*, ALM LJM e-Discovery Law & Strategy (Nov. 1, 2005) <www.lawjournalnewsletters.com/issues/ljm_ediscovery/2_7/news/145513-1.html> (subscription required); Robert D. Brownstone, *Metadata: To Scrub or Not To Scrub; That is the Ethical Question*, Cal. B.J. (Feb. 2008) <<http://Metadata-MCLE-2-1-08.notlong.com>>.

⁶⁰ *Krumwiede v. Brighton Assocs.*, No. 05 C 3003, slip op. at 2006 WL 1308629 (N.D. Ill. May 8, 2006) (entering default judgment for breach of non-compete against a former employee based on metadata showing the employee had deleted and altered thousands of files during delay to produce company-provided laptop), *enforced*, 2006 WL 2349985 (N.D. Ill. Aug. 9, 2006). *Cf.* *Kucala Enters., Ltd. v. Auto Wax Company, Inc.*, 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. May 27, 2003), *aff'd in part and rev'd in part*, 2004 U.S. Dist. LEXIS 5723 (N.D. Ill. Apr. 6, 2004) (dismissing with prejudice based in part on eleventh hour deletion of 12,000 files) <https://ecf.ilnd.uscourts.gov/cgi-bin/show_case_doc?127,119915,....,137,1>.

revisions that could come back to haunt the sender.⁶¹ In addition to the typical over-saving of active files, “[s]taggering quantities of deleted file fragments lodge in the space freed up by deletion, called unallocated space, and even in parts of the unallocated space reoccupied by new files, called slack space.”⁶²

Yet all computer users are subject to the nuances of word processing and spreadsheet files.⁶³ In *Williams v. Sprint*,⁶⁴ plaintiffs brought a class action reduction-in-force (RIF) case based on allegations of age discrimination. Relatively late in the discovery process, the parties stipulated in open court that the employer would produce thousands of Excel spreadsheets in native format. The stipulation did not authorize the employer to scrub metadata or lock cells in the spreadsheets. Yet the employer unilaterally took both actions before producing the spreadsheets in electronic form. It did not make a log of its activities. The court ruled that, in the context of meet-and-confer discussions as to production in native file formats, metadata *is* to be produced even if not specifically sought in the request for production.⁶⁵

In that factual situation, since the beginning of the lawsuit the class of Plaintiffs had alleged that Defendant had, based upon workers’ ages, re-worked employee pools to improve distribution so as to pass adverse-impact analysis. Hence, the relevance of the spreadsheets’ metadata included: the content of changes; the dates of changes; the identities of individuals who had made changes; and any other metadata useable to determine the relative contents of drafts and final versions of the respective files.

Thus, absent first making a timely objection, the producing party’s conduct was disingenuous. Though it knew it had to produce in native format, at the eleventh hour, it unilaterally decided to scrub metadata and to lock formulas.

⁶¹ See generally Schultz, *supra* note 59; see also Tom Zeller Jr., *Beware Your Trail of Digital Fingerprints*, N.Y. Times (Nov. 7, 2005) <<http://Metadata-NYT-11-7-05.notlong.com>> (quoting <<http://www.un.org/news/dh/docs/mehlisreport>>); Stephen Shankland, *Hidden text shows SCO prepped lawsuit against BofA, c/net* (Mar. 18, 2004) <http://news.com.com/2102-7344_3-5170073.html?tag=st.util.print>; Brian Bergstein, *Cos., gov’t seek to keep lid on metadata* (AP 2/3/06) <<http://Bergstein-AP-2-3-06.notlong.com>>; Dennis Kennedy, Evan Schaeffer and Tom Mighell, *Mining the Value from Metadata*, Fios Thinking eDiscovery Column (Jan. 2006) <http://web.archive.org/web/20070804082554/http://www.discoveryresources.org/04_om_thinkingED_0601.html>; Gene Koprowski, *Networking: Not-so-secret documents*, UPI (Feb. 6, 2006) <<http://www.physorg.com/news10567.html>>.

⁶² Craig Ball, *Can Your Old Files Come Back to Life?* Law Tech. News (Jan. 15, 2004) <http://www.law.com/special/supplement/e_discovery/old_files.shtml>; Tom Coughlin, *“Rumors of My Erasure Are Premature”* (Coughlin Associates 2003) <<http://Coughlin-Delete.notlong.com>>; James M. Rosenbaum, *In Defense of the DELETE Key*, 3 GREEN BAG 2D 393, 393-95 (2000) <http://www.greenbag.org/rosenbaum_deletekey.pdf>.

⁶³ See, e.g., Diane Karpman, *Metadata Can Bite You Where It Hurts*, Law-wise, Cal. Bar J. (Nov. 1, 2005), at 20 <<http://Metadata-CalBJ-11-1-05.notlong.com>>; Workshare Commentary, *supra* note 59.

⁶⁴ See 230 F.R.D. 640 (D. Kan. 2005).

⁶⁵ *Id.* at 653–54.

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 <<http://www.archive.org/index.php>>.

II. MONITORING OF EMPLOYEES' ELECTRONIC ACTIVITIES

A. Introduction

The most publicized workplace monitoring issue in recent years has been the surveillance of employee use of e-mail systems and Internet connections. For a number of years, some companies have attracted attention for zero-tolerance policies on personal Internet use by their employees.⁶⁶

A 2006 survey released by the American Management Association⁶⁷ indicated that: 26% of employers have terminated employees for e-mail misuse, 2% have dismissed workers for inappropriate instant messaging (IM) chat; and 2% have fired workers for offensive blog content (including posts on employees' personal home-based blogs). Employers may have a number of legitimate reasons to monitor computer use:

- Abuse of Internet access privileges can result in a substantial drain on workplace productivity, as employees engage in web-surfing instead of their job duties;⁶⁸
- Computer misuse consumes company resources such as bandwidth;⁶⁹
- Disloyal employees may use e-mail to transmit proprietary information from the employer's computer system to a competitor's;⁷⁰
- Transmission of e-mail containing offensive content may give rise to lawsuits for discrimination, harassment or other online torts against the employer;
- Employers face potential liability for criminal acts of employees;⁷¹

⁶⁶ See, e.g., Michelle Conlin, *Workers, Surf at Your Own Risk*, Bus. Wk. (June 12, 2000), at 105.

⁶⁷ See American Management Association and ePolicy Institute, *2006 Workplace E-Mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators* <http://www.amanet.org/press/amanews/2006/blogs_2006.htm/>.

⁶⁸ See *id.* (recounting that one "high-level executive" would spend eight hours a day viewing pornographic content on the World Wide Web) .

⁶⁹ See Jay Kesan, *Cyber-Working or Cyber-Shirking? A First Principles Examination of Electronic Privacy in the Workplace*, 54 Fla. L. Rev. 289 (2002) (estimating misuse may waste up to 60 percent of a company's bandwidth).

⁷⁰ See *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000) (affirming criminal conviction).

- Employers may be liable for employee’s unlawful appropriation of co-worker and client personal information.

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.

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. Those five respective issues are discussed below *seriatim*.

1. Federal Electronic Communications Privacy Act (Wiretap And Stored Communications Act)

The federal Electronic Communications Privacy Act of 1986 (“ECPA”) is an amalgam of Congressional legislation from 1968, 1986 and 2001. Title I of the ECPA, known as the Wiretap Act, , protects information that is in transit. Title II of the ECPA, known as the Stored Communications Act (“SCA”), protects information once it has been received and is at rest, *i.e.*, in storage.⁷²

The ECPA controls the access, use, disclosure, interception and privacy protections related to written and oral electronic communications.⁷³ The ECPA prohibits the acquisition or disclosure of the content of a wire, oral, or electronic communication using electronic, mechanical, or other device.⁷⁴

⁷¹ See generally, Erin M. Davis, *The Doctrine of Respondeat Superior: An Application to Employers’ Liability for the Computer or Internet Crimes Committed by Their Employees*, 12 Alb. L.J. Sci. & Tech. 683 (2002). But see *Butera & Andrews v. International Business Machines Corp.*, No. 1:06-CV-647, 2006 U.S. Dist. LEXIS 75310 (D.D.C. Oct. 18, 2006) <https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2006cv0647-14>, where a law firm – whose e-mail system had been hacked – brought a CFAA claim against the unidentified hacker’s employer. The court granted the Defendant-employer’s motion to dismiss, stating that “an employer cannot be held liable for its employees’ intentional conduct solely on the basis of an employer-employee relationship.” *Id.* at *20. Plaintiff had not alleged the attacks were committed either to further the employer’s interest or in the hacker’s capacity as an employee. *Id.* at *22.

⁷² As to the ECPA generally, see Robert Brownstone and Christine Vogeley, *USA-PATRIOT Act Impasse: Email Interception Rules Need Congressional Attention, Too*, ALJ L.J.N., Vol. 1, No. 2 (Mar. 2006) <http://www.fenwick.com/docstore/Publications/Litigation/Privacy_0306_LJN.pdf>.

⁷³ 18 U.S.C. §§ 2510-2520.

⁷⁴ 18 U.S.C. § 2511(1).

The Wiretap Act applies to the “interception” of a communication, *i.e.*, contemporaneous with its transmission, thereby prohibiting the intentional interception of electronic communications, including e-mail in transit, but not in storage (*i.e.*, in an e-mail inbox).⁷⁵ There are, however, two exceptions: (1) where email is intercepted in the ordinary course of business,⁷⁶ and (2) where there is express or implied consent by at least one party to the communication.⁷⁷

While in 1968 the original Wiretap Act did not initially apply to electronic communications in storage, in 1986 it was amended by the SCA to include stored electronic communications within the scope of the broader ECPA.⁷⁸ The SCA prohibits the intentional unauthorized access of e-mail in storage.⁷⁹ One exception, however, applies to service providers who are exempt when accessing stored electronic information.⁸⁰

With the SCA, Congress relaxed the level of protection for stored communications, divining a lower expectation of privacy in completed transmissions than in “live” conversations. Accordingly, while the SCA generally prohibits unauthorized access to stored email, it provides an exemption for ISPs, which may need to access users’ emails for a variety of legitimate purposes. Therefore, unless email is protected under the SCA’s cohort, namely the Wiretap Act, ISPs will be granted free license to read any email, even before it has been read by the intended recipient.⁸¹

The archaic language of two key Wiretap Act definitions was crafted long before email and is thus unsuited for modern reality. The inherent ambiguity has caused a debate in which the First and Ninth Circuits have taken opposite sides.

In 2001, Congress hastily passed the USA-PATRIOT (“Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism”), Act. One of the Act’s provisions re-defined the Wiretap Act language at the heart of the above-mentioned circuit split. That change not only failed to help matters, but it also led to yet another Wiretap Act case law oddity. The Ninth and First Circuits have purported to apply the pre-USA-PATRIOT version of the ECPA. Yet, paradoxically, each of those courts’ conflicting decisions has relied on the USA-PATRIOT changes as supporting its own view on the interception issue.

In short, the murkiness of the case law in this area – discussed in some detail below – warrants clear, specific policies in the employment setting.

⁷⁵ 18 U.S.C. § 2510(8).

⁷⁶ 18 U.S.C. § 2511(2)(a)(i).

⁷⁷ 18 U.S.C. § 2511(2)(d).

⁷⁸ 18 U.S.C. § 2701.

⁷⁹ *Id.*

⁸⁰ 18 U.S.C. § 2701(c)(1).

⁸¹ See *Hilderman v. Enea Teksci, Inc.*, 551 F. Supp. 2d 1183 (S.D. Cal. 2008).

a. Wiretap Act as Applied to E-Mails in Transit
(i) Majority View – Interception Must be Contemporaneous with Transmission

In 2002, the Ninth Circuit, in *Konop v. Hawaiian Airlines, Inc.* (“*Konop II*”),⁸² joined the group of courts imposing a contemporaneity requirement.⁸³ Robert Konop, a Hawaiian Airlines pilot, maintained a secure website, where he posted discussions criticizing his employer. He authorized fellow employees to access the website via a password and a non-disclosure agreement designed to keep the information from falling into his employer’s hands. Two other pilots allowed the employer to access the website using their login names and passwords. In this manner, Hawaiian’s Vice President accessed Konop’s website over 30 times. Konop subsequently filed suit, alleging violations of the Wiretap Act and SCA, among other claims.

The district court granted summary judgment on the two ECPA claims. On appeal, the Ninth Circuit initially reversed, rejecting the theory requiring contemporaneity.⁸⁴ Then, it withdrew its opinion *sua sponte* and affirmed the district court. In its second opinion, the Ninth Circuit upheld the dismissal of Konop’s claim under the Wiretap Act, but barely maintained his claim under the SCA.

At issue was whether the meaning of “intercept” differed with respect to wire and electronic communications. The court relied upon the earlier Wiretap Act decisions to determine that Congress intended the definition of “intercept” to require acquisition contemporaneous with transmission. Through the ECPA, Congress had ostensibly rescinded the contemporaneousness requirement with respect to wire communications. By altering the definition of “wire communications” to explicitly include stored communications. But it had not done so as to the definition of “electronic communications.”

Comparing the separate definitions, *Konop II* determined, as had previous courts, that Congress had intended the Wiretap Act to protect stored wire communications but not stored electronic communications. By its very nature, a stored wire communication cannot be intercepted contemporaneous with transmission; thus, the requirement was eliminated. Therefore, *Konop II* concluded that “intercept” means two different things for wire and electronic communications. For wire communications, the interception need not be contemporaneous. For electronic communications, the interception must be contemporaneous with transmission.

The Ninth Circuit held that interception of information on Konop’s website had not been contemporaneous. The data on the site had been stored on the server at the time Hawaiian accessed it. In that stored electronic communications were not protected by the Wiretap Act, there could be no interception, and thus no violation, thereunder.

⁸² 302 F.3d 868 (9th Cir. 2002) <<http://KonopII-9thCir-8-23-02.notlong.com>>.

⁸³ See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *U.S. v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003), *cert. denied*, 123 S. Ct. 2120 (U.S. 2003); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 459-60 (5th Cir. 1994). See also Robert D. Brownstone, 9 *Data Security & Privacy Law*, Privacy Litig. Ch. § 9:45 (West 2008).

⁸⁴ *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001) (“*Konop I*”).

The court also opined that protecting stored electronic communications under the Wiretap Act would render the SCA meaningless. Congress intended the SCA to offer less protection to certain stored communications, allowing law enforcement officers to meet a lesser burden than under the Wiretap Act to access such communications. However, if stored electronic communications were to also be protected by the Wiretap Act, law enforcement could never benefit from that lesser burden.

As to whether the employer's conduct had violated the SCA, *Konop II* remanded on a narrow factual issue. In addition to the provider exception, the SCA affords an exemption from liability if access is user-authorized. Two of Konop's fellow pilots had allowed the employer to access the site using their authorized login information. A question remained, however, whether those two pilots qualified as "users" because they had never actually logged on to the website themselves.

(ii) Newer Minority View – Interception need NOT be Contemporaneous with Transmission

The First Circuit performed its own flip-flop on the e-mail interception issue in *U.S. v. Councilman*.⁸⁵ In contrast with the Ninth Circuit, the First Circuit initially found no Wiretap Act violation but then, in its second decision, found that there was a tenable violation. Though purporting to sidestep the contemporaneousness controversy, *Councilman II* implicitly rejected a contemporaneity requirement.

Bradford Councilman ran Interloc, an online rare book listing service. Interloc also provided its book dealer customers with email addresses and acted as their service provider in that regard. Councilman instructed his employees to write a computer program that would intercept and create copies of all e-mail sent from Amazon.com to Councilman's customers. The copies were routed to Councilman's mailbox so that he could read them to gain a commercial advantage. Based on thousands of such e-mail interceptions, Councilman was criminally charged with conspiracy to violate the Wiretap Act. The district court denied a motion to dismiss the indictment.⁸⁶ On appeal in 2004, in its first look at the case, the First Circuit affirmed the dismissal.⁸⁷ The Government successfully sought a rehearing *en banc*. Upon reconsideration, the First Circuit reversed and remanded, potentially reinstating the charge.

After consulting the legislative history, *Councilman II* concluded that the previous interpretations of the Wiretap Act had been inconsistent with Congress' intent. In direct contrast to the Ninth Circuit, the Court held that emails in transit, though also temporarily in storage, were protected by the Wiretap Act.

The *Councilman II* decision first looked to the plain meaning of § 2510. It concluded that the absence of "stored communications" in the definition of "electronic communication" did not necessarily evince Congressional intent to exclude stored messages from protection.

⁸⁵ *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (*en banc*) ("*Councilman II*") <www.ca1.uscourts.gov/pdf/opinions/03-1383EB-01A.pdf>

⁸⁶ *U.S. v. Councilman*, 245 F. Supp 2d 319 (D. Mass. 2003).

⁸⁷ *U.S. v. Councilman*, 373 F.3d 197, 203 (1st Cir. 2004) ("*Councilman I*").

Different canons of construction could manipulate an outcome on either side of the issue and therefore did not resolve the question.

The court thus looked beyond the canons of construction to the legislative history to ascertain Congress' intent when adding electronic communications to the Wiretap Act in 1986. The legislative history showed that the ECPA amended the Wiretap Act to bring electronic communications within its aegis. In addition, Congress had added a clause to the definition of "wire communication" to protect wire communications in storage. The legislative history had specifically referenced voicemail as an example. The *Councilman II* majority concluded that the sole reason for the new clause was to include voicemail under the Wiretap Act, not to exclude email.

In fact, the legislative history indicated that "interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties."⁸⁸ *Councilman II* thus concluded that "the purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections."⁸⁹ Accordingly, the court rejected the notion that transient electronic communications temporarily in storage are not "electronic communications."

The *Councilman II* majority averred that it was only looking at the "wire" and "electronic" communications definitions and that it was not touching on contemporaneity. However, the majority opinion concluded with dicta on the "intercept": concept, finding it "impossible" for defendant to show an e-mail transmission had been completed while the message was still "en route."⁹⁰

All of the Councilman decisions were written after the USA-PATRIOT Act's October 2001 amendment of the "wire communications" definition – namely the removal of "storage." Yet the events precipitating the Councilman prosecution had occurred before October 2001. Thus, like *Konop II* before it, *Councilman II* was bound to interpret and apply the pre-PATRIOT version of the Wiretap Act. However, also akin to *Konop II*, *Councilman II* nonetheless infused its "intercept" analysis with its own spin on the 2001 Congressional action.

In October 2001, the USA-PATRIOT Act § 209 amended the Wiretap Act by eliminating storage from the definition of "wire communication." Given the timing of the underlying facts, *Konop II* and *Councilman II* were supposed to apply pre-USA-PATRIOT statutory and case law. However, both those decisions discussed PATRIOT's elimination of "storage" from the "wire communication" definition. Strikingly, however, the Ninth Circuit and First Circuit each drew a different inference. *Konop II* interpreted the 2001 amendment to indicate that neither stored wire communications nor electronic communications are protected. In other words, an interception must always be contemporaneous with transmission to constitute a Wiretap Act violation. As noted above, *Councilman II* drew a contrasting inference, finding that the temporary storage of email in transit does not exclude it from protection under the Act.

⁸⁸ 418 F.3d at 76.

⁸⁹ *Id.*

⁹⁰ *Id.* at 79.

To date, no published decision appears to have addressed a post-October-2001 factual scenario in this context. Thus, apparently no court has confronted the issue of how or whether the amendment changes the interpretation of the Wiretap Act. Regardless, § 209 is among several provisions of the PATRIOT Act renewed by Congress on March 2, 2006. While reviewing the 16 expiring USA-PATRIOT Act provisions, unfortunately Congress did not focus substantively on § 209 at all. Nor, since then, has Congress acted on a piece of legislation that would have brought clarity to the “intercept” issue.⁹¹

Again, in the workplace context, the need for clear-cut written policies is paramount.

b. Stored Communications Act as Shield and Sword

(i) Shield: Employer Access to Stored E-mails, “Private” Web-Based E-mail Systems, Pagers and Employee Web Sites

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.⁹² 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.⁹³

⁹¹ S. 936, *E-mail Privacy Act of 2005* <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s936is.txt.pdf>.

⁹² See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff’d on other grounds*, 352 F.3d 207 (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 (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).

⁹³ *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879–80 (9th Cir. 2002), *cert. denied*, 2003 WL 397601 (U.S. 2003) (“*Konop II*”) (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*, 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.*

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.⁹⁴ Many of these employees may not realize that such activity leaves electronic footprints on the hard drives of company-issued computers. Nor are many employees likely aware that commercially available software allows employers to monitor, keystroke by keystroke, the text they type into these pages.⁹⁵

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 is written).

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. However, to avoid any arguments premised on a “reasonable expectation of privacy,” employers may want to emphasize, in their policies on Internet and e-mail use that communications sent through third-party e mail services are equally subject to monitoring.⁹⁶

⁹⁴ At times, an “e-sabotage” scenario ensues whereby a corporate insiders uses a third-party e-mail services to transmit confidential information from his or her employers’ computer systems.

⁹⁵ See, for example, the publicity materials for the “Spector” software package <<http://www.spectorsoft.com/>>.

⁹⁶ See, e.g., *Sims v. Lakeside School*, 2007 WL 2745367, 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. Sept. 20, 2007) (“unequivocally clear [contents of] policy on computer networks” partially trumped by “public policy” such that employer “not permitted to review any webbased generated e-mails, or materials created by plaintiff . . . to communicate with his counsel or his wife”); *Curto v. Medical World Communic., Inc.*, 2006 WL 1318387, 99 Fair Empl. Prac. Cas. (BNA) 298 (E.D.N.Y. May 15, 2006) (ex-employee had not waived privilege or work product immunity as to information recovered forensically from work-at-home laptop provided by employer) (*distinguishing U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000)); *Nat’l Econ. Research Assocs. (NERA) v. Evans*, 2006 Mass. Super. LEXIS 371, 21 Mass. L. Rep. 337 (Mass. Super. Ct. 2006) (“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.”); *People v. Jiang*, 31 Cal. Rptr. 3d 227 (Cal App. 6 Dist. 2005) (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”). See also *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 251, 259 (Bankr. S.D.N.Y. 2005) (“[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”). 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).

Such arguments occasionally 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.⁹⁷ The most recent decision on this issue accepted the employee's privilege argument, thereby reversing the trial court's determination.⁹⁸

Remember, though, that 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.⁹⁹

⁹⁷ See note 96 *supra*. 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/valawyer magazine/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 Privacy & Security Law Report No. 18, at 685 (May 5, 2008) <<http://pubs.bna.com/ip/bna/pvl.nsf/eh/a0b6k4w6m5>>. 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"); *Scott v. Beth Israel Medical 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; finding Plaintiff's communications with attorney regarding litigation, transmitted over Defendant's email system, not protected by attorney-client privilege or work-product, in light of "no personal use" e-mail policy combined with stated policy allowing for employer monitoring).

⁹⁸ *Stengart v. Loving Care Agency, Inc.*, 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. June 26, 2009) ("[f]inding that the policies undergirding the attorney-client privilege substantially outweigh the employer's interest in enforcement of its unilaterally imposed regulation, we reject the employer's claimed right to rummage through and retain the employee's emails to her attorney") <<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>>. The appellate court decision is discussed in Dubé, Lawrence E., *Employer Cannot Copy Worker's E-Mails To Lawyer Sent From Company Laptop*, BNA PSLR (July 6, 2009), available by subscription at <http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=13739951&vname=pvlrnotallissues&fcn=7&wsn=498740000&fn=13739951&split=0>. The now-reversed lower court decision is 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) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428912956&rss=ltm>>.

⁹⁹ See notes 100-116, 208-14 and 302-323 and accompanying text below.

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.¹⁰⁰ Very recently, one federal circuit found that, as a result of such unlawful access, actual damages and/or punitive damages may be recoverable.¹⁰¹

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 wide-ranging Circuit Court opinions.¹⁰² One of those decisions was retracted and then undone by an *en banc* decision by the Sixth Circuit.¹⁰³

However, the second such decision, by the Ninth Circuit in *Quon v. Arch Wireless Op. Co.*,¹⁰⁴ is an important cautionary tale as to the disastrous consequences of: 1) not only failing to update old policies to comport with technology advances; 2) but also allowing inconsistent “operational reality” to trump the contents of a technology-use policy.¹⁰⁵ In *Quon*, police officer Quon brought SCA and Fourth Amendment 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.¹⁰⁶

¹⁰⁰ See *Van Alstyne v. Electronic Scriptorium, Ltd.*, 560 F.3d 199, 28 IER Cases 1441 (9th Cir. 2009) <<http://pacer.ca4.uscourts.gov/opinion.pdf/071892.P.pdf>>. See also footnote 93 supra (discussing *Konop* and *Fischer*).

¹⁰¹ *Van Alstyne v. Electronic Scriptorium, Ltd.*, 560 F.3d 199, 28 IER Cases 1441 (9th Cir. 2009) <<http://pacer.ca4.uscourts.gov/opinion.pdf/071892.P.pdf>>. See also Ralph Losey, New 4th Circuit Ruling on Illegal e-Discovery Adds Teeth to Federal Anti-Hacker Email Privacy Law, e-Discovery Team Word Press (Mar. 29, 2009) <<http://ralphlosey.wordpress.com/2009/03/29/new-4th-circuit-ruling-on-illegal-e-discovery-adds-teeth-to-federal-anti-hacker-email-privacy-law/>>, Marcia Coyle, *Landmark Ruling in E-Mail Theft Case*, Nat'l L. J. (Mar. 26, 2009) <<http://www.law.com/jsp/ca/PubArticleFriendlyCA.jsp?id=1202429394819>>.

¹⁰² *Warshak v. U.S.*, 490 F.3d 455, 472-73 (6th Cir. 2007) (distinguishing *U.S. v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) from *U.S. v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007)) <<http://www.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) <<http://www.ecommercetimes.com/story/SP5NFpwQVKGgS1/Carving-Out-New-Privacy-Rights-for-E-Mailers.xhtml#>>.

¹⁰³ *Warshak v. U.S.*, 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>>.

¹⁰⁴ 529 F.3d 892 (9th Cir. 2008).

¹⁰⁵ *Id.* at 907.

¹⁰⁶ See Fenwick & West LLP, *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 *Quon* is partially based.

Quon had signed an employer policy that prohibited personal use of e-mail and warned that employees "should have no expectation of privacy or confidentiality when using [City electronic] resources."¹⁰⁷ 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 city employee 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 that exceeding the maximum usage for which the City would pay.¹⁰⁸ Ultimately, Quon indeed paid for overages on several occasions.

Later, management audited Quon's messages and found many personal, sexually explicit messages. The court opined that if the employer had followed its written policy, then Quon would have had no expectation of privacy in his pager use.¹⁰⁹ However, the city administrator's statements and *modus operandi* combined with Quon's overages payments effectively vitiated the policy and created an expectation of privacy for Quon under the Fourth Amendment in his use of the pager to send and receive personal text messages.¹¹⁰

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 to be held.¹¹¹ The majority opinion in *Quon II* noted the informal policy was express and specific: employees were to reimburse the city for any usage in excess of 25,000 characters but usage would not be audited.¹¹² In other words, under the informal policy effectuated by Quon's supervisor, text messages' contents and recipients' identities were to remain confidential¹¹³

Finally, the underlying purpose of the audit of Quon's pager records was not to uncover any purported misconduct but rather to determine whether the city should change its usage rates. Thus, the City had no legitimate purpose in its search to overcome Quon's reasonable expectation of privacy in his City-issued pager.

A vehement dissenting opinion contended that the majority had departed from Supreme Court precedent to the effect that the "operational realities of the workplace make

¹⁰⁷ *Quon v. Arch Wireless Op. Co.*, 529 F.3d 892, 896, 906 (9th Cir. 2008) ("*Quon I*").

¹⁰⁸ *Id.* at 897, 906-09.

¹⁰⁹ *Id.* at 906-08

¹¹⁰ *Id.*

¹¹¹ *Quon v. Arch Wireless Op. Co.*, 2009 WL 224544, at *2-*5 (9th Cir. Jan. 27, 2009) ("*Quon II*"), also available at <http://www.ca9.uscourts.gov/datastore/opinions/2009/01/27/0755282c.pdf>.

¹¹² *Id.* at *3.

¹¹³ *Id.*

some employees' expectations of privacy unreasonable."¹¹⁴ The majority countered that they had appropriately adhered to that same judicial precedent's mandate of a case-by-case approach. According to the majority, an analysis of the underlying factual circumstances warranted a finding that Quon's constitutionally protected privacy interest had overcome the necessity of the audit.¹¹⁵

Of particular interest to public sector entities and their counsel is the heated debate between the two *Quon II* opinions as to the true meaning of *O'Connor v. Ortega*, 480 U.S. 709 (1987) as to employer searches of employees. In particular, the dissent accused the majority of inaptly applying a "less intrusive means" standard. The factions could not agree on whether the underlying search was of the "special needs" or "investigatory" variety. Moreover, their interpretations varied of the factual record as to the breadth of the uses to which the officers were supposed to put the pagers.

The upshot of the now validated June 2008 *Quon* opinion is that, absent the presence of both a clear-cut policy and in-the-trenches practices to the contrary, the door can be open for employees to establish an expectation of privacy when using an employer's resources. Although *Quon* involved a public sector employment relationship arguably intertwined with a police investigation where Fourth Amendment rights exist, it is impactful for both public and private employers in its reminder of the importance of: (1) keeping policies up to date and; (2) avoiding statements and practices at variance with official written policies.

Employers should recognize that their access to third-party services is most likely limited to monitoring "real-time" data transmitted over the employers' own Internet connections, as in *Konop II*, discussed in detail in Section II(B)(1)(a)(i) above.¹¹⁶

(ii) Sword: Affirmative Claim Based on Snooping by Former Employee

On the other hand, the SCA may be a useful sword in the situation in which, after separating from the company, a former employee gains illicit access to the employer's e-mail system. In October 2008, the Middle District of Tennessee, in *Cardinal Health 414, Inc. v. Adams*, deemed an SCA claim viable based on a former employee's underhanded use of his former co-worker's log-in information to spy on the activities of his former employer to benefit a competitor.¹¹⁷

¹¹⁴ *Quon v. Arch Wireless Operating Co.*, 2009 WL 224544, at *6-11 (9th Cir. Jan. 27, 2009) (dissent), also available at <<http://www.ca9.uscourts.gov/datastore/opinions/2009/01/27/0755282d.pdf>>.

¹¹⁵ *Id.* at 3.

¹¹⁶ *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") <[www.ca9.uscourts.gov/ca9/newopinions.nsf/AE0DB21CF9CC371A882572B3007EB140/\\$file/0510322.pdf?openement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/AE0DB21CF9CC371A882572B3007EB140/$file/0510322.pdf?openement)>.

¹¹⁷ *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 970-971 (M.D. Tenn. 2008)

As *Adams* noted, to be liable under the SCA, Defendant must have intentionally accessed unauthorized material.¹¹⁸ There, Adams had admitted to intentionally and knowingly accessing his former employer's email system and providing the information to a direct competitor. In his defense he argued his access had been authorized because he was given his former co-worker's user name and password.¹¹⁹ Adams analogized his case to *Sherman & Co v. Salton Maxim Housewares, Inc.*,¹²⁰ where the former employee's use of his personal log-in to access a business account did not violate the SCA. *Sherman* had faulted the company for not having adopted clear and explicit restrictions on former employees' access.

Unlike *Sherman*, Adams used another person's log-in information to spy on his former company's activities. Thus, where the facts indisputably presented a case of Adams logging into another's email account without knowledge or permission of the account holder and reviewing the material therein, summary judgment of the SCA violation was appropriate.¹²¹

While the SCA punishes the unauthorized act of accessing a "facility through which an electronic communication service is provided," the SCA does *not* punish the use and disclosure of the information obtained.¹²² In *Adams*, the employer contended that the emails shared with a competitor had contained profit and loss statements, customer pricing information and other private and confidential information. By way of rebuttal, Adams insisted the information was "gossip" that contained no "confidential or proprietary" information.¹²³

Either way, the record reflected that, during the period of unauthorized access, his former employer had lost business to the competitor with which Adams was in cahoots.¹²⁴ However, the competitor's acceptance and use of the material did not constitute "access." Consequently, even though the competitor had used the information to gain a business advantage, it was not liable under the SCA.

The take-home message is clear. To avoid former employees' unauthorized access to stored information, a company should not only systematically require periodic password updates but also discontinue log-in access upon each employee's departure.

¹¹⁸ *Id.* at 976 (discussing *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004) ("unauthorized access" under SCA akin to trespass to property)).

¹¹⁹ *Adams*, 582 F. Supp. 2d at 978.

¹²⁰ 94 F. Supp. 2d 817 (E.D. Mich. 2000) .

¹²¹ *Adams*, 582 F. Supp. 2d at 976.

¹²² *Id.* (finding Section 2701(a) of the EPCA does not expressly prohibit the disclosure or use of the information gained without authorization.)

¹²³ *Adams*, 582 F. Supp. 2d at 972-73.

¹²⁴ *Id.* at 972.

2. State Analogues to the ECPA

Since the ECPA does not preempt the field of monitoring of electronic communications, several states, including California,¹²⁵ have enacted more stringent restrictions regarding the interception of wire and electronic communications.

Only two states have regulated employers' monitoring of e-mail. A Connecticut statute prohibits monitoring without notice to employees.¹²⁶ Delaware law permits employers to monitor employee e-mail and Internet usage upon giving a one-time notice which is acknowledged by the employee either in writing or electronically.¹²⁷ State laws providing greater protections for e-mail privacy, like statutes providing greater protections for telephone calls, would not be preempted. However, given the wide dispersion of e-mail servers and clients on a computer network, serious issues of comity among several states may be raised by patchwork regulation of this field by different states.

Most state laws mirror the ECPA and therefore similarly do not prohibit employer monitoring of e-mail.¹²⁸ Courts have generally rejected claims of invasion of privacy brought by employees whose e-mail has been intercepted by their employers. In one case, a federal court in Pennsylvania rejected state-law privacy claims against an employer that had intercepted e-mail messages containing disparaging comments about a supervisor.¹²⁹ Interestingly, the court placed little weight on the company's assurances to its employees that it would respect the privacy of e-mail communications.¹³⁰ However, a state trial court in

¹²⁵ See Cal. Penal Code § 631, *et. seq.*

¹²⁶ Conn. Gen. Stat. § 31-48d.

¹²⁷ Del. Code Ann. Tit. 19 § 705. See generally Brownstone, Robert D., 9 *Data Security & Privacy Law, Privacy Litig.* Ch. § 9:45-9:46 (West 2008) .Hooper, Carey C., "You've Got Mail": *Privacy Rights in the Workplace*, 25 S. Ill. U.L.J. 609, 625-26 (2001); Isajiw, Peter, J., *Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 Temp. Envtl. L. & Tech. J. 73, 90-92 (2001) (discussing several of the state wiretap statutes).

¹²⁸ Some years ago, a trial court in California ruled that the California Invasion of Privacy Act, Cal. Penal Code §§ 630-637.9 does not protect against eavesdropping on e-mail. *Shores v. Epson Am., Inc.*, No. BC007036 (Cal. Super. Ct. Mar. 12, 1991). That court rejected an employee's claim that her employer's acts of routinely printing out all electronic mail that company employees exchanged with people outside the company violated California's Invasion of Privacy Act. See also Jennifer J. Griffin, *The Monitoring of Electronic Mail in the Private Sector Workplace and Electronic Assault on Employee Privacy Rights*, 4 *Software L.J.* 493 (1991).

¹²⁹ See *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1997); see also *McLaren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103 (Dallas May 28, 1999) (rejecting invasion of privacy claim when management accessed employee "personal" folders on company computers).

¹³⁰ *But see Rulon Miller v. International Business Machines Corp.*, 162 Cal. App. 3d 241, 208 Cal. Rptr. 524 (1984) (wrongful discharge and emotional distress claims upheld when employee fired for romantic relationship with a competitor's employee; company policy stated respect for employees' private lives), *overruled on other grounds*, *Guz v. Bechtel Nat'l, Inc.*, 24 Cal. 4th 317 (2000).

Massachusetts allowed an employee's invasion of privacy claim to proceed where the employer had not warned that it was monitoring e-mail.¹³¹

To protect against constitutional and common law 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.¹³²

In addition, cautious employers may wish to monitor e mail only when a legitimate business interest exists to do so.¹³³ Yet, many employers, especially in high technology fields, routinely monitor e-mails to insure against the transmission of trade secrets to a competitor.

However, 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 "NLRB" 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.¹³⁴ The D.C. Circuit's recent decision 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.

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

¹³¹ *Restuccia v. Burk Tech.*, 1996 Mass. Super. LEXIS 367 (1996).

¹³² Requiring employees to give written consent to the monitoring of e mail will normally vitiate common law privacy claims. Prosser, William L. & Keeton, Robert E., *Prosser & Keeton on Torts* § 112 (5th ed. 1984).

¹³³ For some time, commentators have suggested that employer efforts to prevent use of e-mail systems for personal non business communications comprise a sufficient business interest to justify monitoring. See, e.g., J. Griffin, *Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee Privacy Rights*, 4 *Software*, L.J. 493, 508 (1991).

¹³⁴ *The Guard Publ'ng Co. d/b/a The Register-Guard and Eugene Newspaper Guild*, 351 NLRB No. 70 (Dec. 16, 2007) <http://www.nlr.gov/shared_files/Board%20Decisions/351/V35170.pdf>, reversing in part and affirming in part, Cases 36-CA-8743-1, *et al.* <http://www.nlr.gov/research/frequently_requested_documents.aspx>.

and Abuse Act (“CFAA”).¹³⁵ Such a cause of action confers federal subject matter jurisdiction, enabling the suit to proceed in federal court.

A CFAA claim may be a desirable supplement to a trade secret action against a disloyal former employee who accessed proprietary information before separating from a company.¹³⁶ 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.¹³⁷ However, as discussed in detail in this sub-section, there is a split in case law as to the viability of the Act’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.¹³⁸ 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

¹³⁵ 18 U.S.C. § 1030.

¹³⁶ 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>. As to the CFAA theory in particular, see Erika Morphy, *The Computer Fraud Act: Bending a Law to Fit a Notorious Case*, E-Commerce Times (12/09/08) (quoting Robert D. Brownstone) <www.ecommercetimes.com/story/65424.html#>.

¹³⁷ Ilana S. Rubel, *Screen Grabs*, Daily J. (3/13/09), available at <http://www.fenwick.com/docstore/Publications/Litigation/Shrinking_Prospects_CFAA.pdf> (last visited July 14, 2009).

¹³⁸ 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 Robert D. Brownstone, 9 *Data Security & Privacy Law*, Privacy Litig. Ch. §§ 9:3 through 9:16 (West 2008).

computer.¹³⁹ As to potential defendants, the category of "violator" under Section 1030(g) may include not only a complete stranger but 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.¹⁴⁰

Currently on the cutting edge is whether a disloyal employee is an apt defendant on a CFAA cause of action brought by his/her (former) employer. 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 at least 26 U.S. district court decisions in this area. The outcomes in those decisions have split evenly, with 13 opinions (six in the Seventh/"*Citrin*" Circuit) for the (ex-) employer/Plaintiff; and 13 (one in the Seventh Circuit) for the (ex-) employee/Defendant, on one ground or another.¹⁴¹

¹³⁹ *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004) (rejecting "ownership or control requirement" that trial court had read into 18 U.S.C.A. §1030(g), where two individuals complained that their e-mails had been improperly obtained from ISP pursuant to "massively overbroad" and "patently unlawful" non-party subpoena served on ISP by their employer's litigation opponent in another lawsuit). *Cf. Garland-Sash v. Lewis*, 2007 WL 935013 (S.D.N.Y. Mar. 26, 2007) (denying in part motion to dismiss CFAA claims brought by inmate's wife who claimed that prison counselor had accessed inmate's visitor record and inappropriately deleted wife's name).

¹⁴⁰ As to the student-hacker context, *see, e.g., U.S. v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (upholding criminal conviction of student hacker; noting that "Courts have . . . typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user"), *cert. denied*, 128 S. Ct. 119, 169 L. Ed. 2d 27 (U.S. Oct. 1, 2007). As to vicarious liability, *see, e.g., Charles Schwab & Co., Inc. v. Carter*, 2005 WL 2369815 (N.D. Ill. 2005) (finding actionable claim for vicarious liability because "[t]o hold otherwise would exempt a principal from liability when its agent improperly accessed a computer at the direction of the principal"); *Binary Semantics Ltd. v. Minitab, Inc.*, No. 4:07-CV-1750, 2008 WL 763575, at *5 (M. D. Pa. Sept. 2, 2008) (denying motion to dismiss CFAA claim against employer where employee had accessed plaintiff's computer to steal trade secrets). *But see Calence, LLC v. Dimension Data Holdings*, 2007 WL 1549495 (W.D. Wash. May 24, 2007) (no basis for CFAA claim because "[P]laintiff points to no evidence in the record that corporate defendants directed either of . . . individual [defendant]s to take any of the alleged improper actions"); *Butera & Andrews v. International Business Machines Corp.*, 456 F. Supp. 2d 104, 112 (D.D.C. Oct. 18, 2006) ("an employer cannot be held liable for its employees' intentional conduct solely on the basis of an employer-employee relationship" unlike here, need an allegation that attacks committed either to further employer's interest or in hacker's capacity as employee).

¹⁴¹ In the Fall of 2008, BNA compiled a chart summarizing some of the opinions on each side of the fence. BNA, Inc., *Meaning of 'Unauthorized Access' Continues to Divide Federal Courts*, 7 Privacy & Security Law Report No. 34, at 1282 (Sep. 1, 2008) <<http://pubs.bna.com/ip/bna/pvl.nsf/eh/a0b6z4v6r6>>. Moreover, last summer, the split in authority caused a Tennessee district court to certify an interlocutory appeal, asking the Sixth Circuit to provide guidance in this uncertain context. *Black & Decker (US), Inc. v. Smith*, 2008 WL 3850825 (W.D. Tenn. 2008) ("*Black & Decker II*"). The underlying *Black & Decker* CFAA decision is discussed in BNA, Inc., *Employee's Misuse of Regularly Available Data Held Not Unauthorized Access for CFAA*, 7 Privacy & Security Law Report No. 30, at 1121 (July 30, 2008) <<http://pubs.bna.com/ip/bna/pvl.nsf/eh/a0b6v9t6n4>>.

Trade secret plaintiffs will often assert a claim under the Act by alleging the defendant did one or more of the following:

- intentionally accessed a computer without authorization or exceeded authorized access, and thereby obtained information from a protected computer;
- knowingly and with intent to defraud, accessed a protected computer without authorization, or exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value;
- knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer;
- intentionally accessed a protected computer without authorization, and as a result of such conduct, intentionally or recklessly caused damage and loss.

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 Seventh Circuit has adopted the plaintiff-friendly view, applying agency principles to the question of authorized access. In *International Airport Centers v. Citrin*,¹⁴² the court revived a CFAA claim against a former employee who had installed a computer program that cleansed his laptop hard drive. The ex-employee's conduct had prevented the recovery of both company data and evidence of the employee's disloyalty. The installation and use of the disk-erasure program constituted were deemed an unlawful "transmission."¹⁴³ The court also found that the employee's actions were "unauthorized": "an employee accesses [employer data] 'without authorization' at the moment the employee acquires a subjectively adverse interest to the employer."¹⁴⁴

¹⁴² *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006), <<http://caselaw.lp.findlaw.com/data2/circs/7th/051522p.pdf>>, on subsequent appeal, 445 F.3d 749 (7th Cir. 2006) <<http://caselaw.lp.findlaw.com/data2/circs/7th/062073p.pdf>>.

¹⁴³ 440 F.3d at 420. *But see Hasan v. Foley & Lardner, LLP*, 2007 WL 2225831, at *4 (N.D. Ill. July 26, 2007) (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>>..

¹⁴⁴ *Citrin*, 440 F.3d at 421. *See also Nilfisk-Advance v. Mitchell*, 2006 WL 827073, at *2 (W.D. Ark. Mar. 28, 2006) (employee exceeded any authorization once he had developed the intent to misappropriate) <https://ecf.arwd.uscourts.gov/cgi-bin/show_case_doc?13,26525,....,52,1>; *Forge Indus, Staffing v. De La Fuente*, 2006 WL 2982139, at *6 (N.D. Ill. Oct. 16, 2006) (any authorization [an operations director] had to delete or erase information from [his work laptop] ended when he engaged in misconduct in violation of his duty of loyalty to the company)

Decisions following this view have sprung up inside and outside the Seventh Circuit.¹⁴⁵

In addition to looking at agency principles, some courts have expanded the limits

<<http://Forge-DeLaFuente-NDIII-10-16-06.notlong.com>>.; *Mintel Int'l Group, Ltd. v. Neergheen*, 2008 WL 2782818, at *3 (N.D. Ill. Jul. 16, 2008) (“exceeded authorized access” allegations sufficient to demonstrate likelihood of success so as to justify TRO against ex-employee); *Motorola Inc. v. Lemko Corp.*, 2009 U.S. Dist. LEXIS 10668 (N.D. Ill. Feb. 11, 2009) (citing *Mintel*, holding that allegations that an employee e-mailed and downloaded confidential information for an improper purpose are sufficient to state a claim that the employee exceeded her authorization) <<https://ecf.ilnd.uscourts.gov/doc1/06706071965>>; *Pac. Aerospace & Elec. v. Taylor*, 295 F. Supp. 2d 1188, 1195-97 (E.D. Wash. 2003); *Calyon v. Mizuho Sec. USA, Inc.*, 2007 U.S. Dist. LEXIS 66051, 2007 WL 2618658, at *1 (S.D.N.Y. 2007); *Shurgard Storage Centers Inc. v. Safeguard Self Storage Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

¹⁴⁵ See generally *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 following *Citrin*) <<https://ecf.ned.uscourts.gov/doc1/11301655270>>; *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 “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>>; *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”); *MPC Containment Systems, Ltd. v. Moreland*, 2008 WL 2875007 (N.D. Ill. Jul. 23, 2008) (pro-employer decision); *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); *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); *Alliance Int'l, Inc. v. Todd*, 2008 WL 2859095 (E.D. N.C. July 22, 2008) (pro-employer decision following *Citrin* and *Forge*); *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) <https://ecf.njd.uscourts.gov/cgi-bin/show_case_doc?pdf_header=0&case_id=169571&doc_num=57&att_num=0&got_receipt=1&de_seq_num=234>.

of “exceeding authorized access” by looking at company policies or agreements.¹⁴⁶

In contrast to decisions within, and agreeing with, the Seventh Circuit, a number of decisions have rejected the plaintiff-friendly view. This other camp has held that access to a protected computer occurs “without authorization” *only* when initial access is not permitted.¹⁴⁷ Those courts have thus ruled that a violation for “exceeding authorized access” occurs only when the access of certain underlying information was not permitted.¹⁴⁸

¹⁴⁶ See *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); *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/cgi-bin/show_case_doc?173.93885.....612,1>; *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (affirming preliminary injunction against competitor tour company; Plaintiff likely to succeed on CFAA’s “exceed[ed] authorized access” element, 18 U.S.C.A. § 1030(a)(4), (e)(6), because competitor’s Vice President breached confidentiality agreement he had signed while previously in Plaintiff’s employ, by using proprietary information to enable “scraper” software program – a/k/a “bot” – to glean two years of prices so his new company could systematically undercut those prices). Cf. *Del Monte Fresh Produce N.A. Inc v. Chiquita Brands Int’l Inc.*, 616 F. Supp. 2d 805, 815 (N.D. Ill. Mar. 19, 2009) (though dismissing CFAA claim, finding viable claim against ex-employee for breach of confidentiality provisions of IT Operations Contract) <<https://ecf.ilnd.uscourts.gov/doc1/06706222648>>.

¹⁴⁷ The most recent decision to so hold was *Vurv Technology LLC v. Kenexa Corp.*, 2009 WL 2171042 (N.D. Ga. July 20, 2009). Other decisions issued this year include *American Family Mut. Ins. Co. v. Hollander*, 2009 U.S. Dist. LEXIS 16897, at *30 (N.D. Iowa Mar. 3, 2009) (explicitly following the *Condux* line of cases: “even if the information obtained was subsequently used for an improper purpose, there is no violation of the CFFA” where, during the course of his employment, Defendant had accessed a database that he was encouraged to utilize) <<https://ecf.iand.uscourts.gov/doc1/0750756276>>; *Bridal Expo, Inc. v. van Florestein*, 2009 WL 255862 (S.D. Tex. Feb. 3, 2009) (pro-employee decision based on lack of “unauthorized” element); *Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing, & Consulting, LLC*, 2009 WL 151687, at *6 (E.D. Mo. Jan. 22, 2009) (dismissing CFAA-related counts because Plaintiff failed to properly allege “without authorization;” citing *Condux* Marketing, & Consulting, LLC, 2009 WL 151687, *6 (E.D. Mo. Jan. 22, 2009) <<https://ecf.moed.uscourts.gov/doc1/10702616802>>; *U.S. Bioservs. v. Lugo*, 2009 WL 151577 (D. Kan. Jan. 21, 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>>.

¹⁴⁸ In addition to the 2009 decisions, see *Condux Int’l, Inc. v. Haugum*, 2008 WL 5244818, *9 (D. Minn. Dec. 15, 2008) (“[t]he interpretation . . . articulated in the *Shurgard/Citrin* line of cases incorrectly focuses on what a defendant did with the information after he accessed it [use of information], rather than on the appropriate question of whether he was permitted to access the information in the first place [use of access.]”); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967-68 (D. Ariz. 2008) (given that employee’s computer access was permitted in the first place, electronically copying important documents to personal e-mail account – though may have wronged company – not “unauthorized” use of); *Arience Builders, Inc. v. Baltes*, 563 F. Supp. 2d 883 (N.D. Ill. 2008) (pro-employer decision); *Resource Ctr. For Independent Living, Inc. v. Ability Resources, Inc.*, 534 F. Supp. 2d 1204, 1211 (D. Kan. 2008) (“the restrictive view of

Not only is there a split among the Circuits but here have also been intra-circuit splits. For example, within the Ninth Circuit, District Courts in California and Washington have followed the *Citrin* view, while the Arizona District Court has rejected it.¹⁴⁹

The second hurdle to bringing a viable action against a current or former

'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.'"); *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929, 934-36 (W.D. Tenn. 2008) ("*Black & Decker I*"); *Winner, Inc v. Polistina*, 2007 WL 1652292, at *5 (D. N.J. June 4, 2007) ("Congress did not intend to create a private cause of action against employees whose crime . . . merely involved the use of ordinary email in a manner disloyal to their employer and in breach of their employment contract.") <<http://Winner-Polistina-DNJ-6-4-07.notlong.com>>.

See also *Diamond Power International Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 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*"); *B & B Microscopes v. Armogida*, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) ("[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'"); *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Masuda*, 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") <https://ecf.mdd.uscourts.gov/cgibin/show_case_doc?pdf_header=0&case_id=123342&doc_num=103&att_num=0&got_receipt=1&de_seq_num=299>; *Secureinfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 609-10 (E.D. Va. 2005) (refusing to find a lack of authorization where licensee gave access to plaintiff's server to defendant in violation of license agreement) <https://ecf.vaed.uscourts.gov/cgibin/show_case_doc?pdf_header=0&case_id=192288&doc_num=156&att_num=0&got_receipt=1&de_seq_num=587>.

¹⁴⁹ Compare *Hanger Prosthetics & Orthotics Inc. v. Capstone Orthopedic Inc.*, (E.D. Cal. 2008), *ViChip Corp. v. Tsu-Chang Lee*, 438 F. Supp. 2d 1087 (N.D. Cal. 2006) and *Shurgard Storage Centers Inc. v. Safeguard Self Storage Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) with *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 963 (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"). There has also been a split within the Middle District of Florida. Compare *Pharmerica, Inc. v. Arledge*, 2007 WL 865510, at *6-8 (M.D. Fla. Mar. 21, 2007) (relying on *Citrin*, *P.C. Yonkers* and *Shurgard* in finding likelihood of success on merits where employee had "duplicate[ed] and cop[ied confidential documents] and/or sending them to his home computer or personal email account and [then] deleting them from [his employer's] computers") with *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058, at *8 (M.D. Fla. Aug. 1, 2006) <<http://Lockheed-Speed-8-01-06.notlong.com>>, reconsideration denied by *Lockheed Martin Corp. v. L-3 Communications Corp.*, 2007 WL 569994 (M.D. Fla. Feb. 20, 2007) (refusing to follow *Citrin*; holding that copying computer files neither "without authorization" nor exceeding authorization" because such access had occurred while employee had still enjoyed access rights to company's computer system).

employee is proving loss and/or damage.¹⁵⁰ 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. At least one decision, however, has reached a different result.¹⁵¹

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.”¹⁵² The majority of courts nationwide, particularly recently, 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

¹⁵⁰ The loss/damage decisions in the disloyal-employee context include *Condux Int’l, Inc. v. Haugum*, 2008 WL 5244818, *9 (D. Minn. Dec. 15, 2008) (“there is no allegation of the ‘damage’ contemplated by the CFAA” from “mere unauthorized copying, downloading, or emailing of confidential or proprietary information”); *Del Monte Fresh Produce N.A. Inc v. Chiquita Brands Int’l Inc.*, 2009 U.S. Dist. LEXIS 22694, *10 (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”); *Andritz Inc. v. S. Maint. Contractor LLC*, 2009 WL 48187, *3 (M.D. Ga. Jan. 7, 2009) (theft and use of trade secrets not actionable “loss” or “damage” under the CFAA because “[a]fter the alleged theft of the data, Plaintiff still had access to the data just as it had before Defendants’ actions; t]he alleged CFAA violation is not that Defendants deleted or altered any data but that Defendants used the data inappropriately”) <<https://ecf.gamd.uscourts.gov/doc1/0530954060>>; *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)”); *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”); *Nexans v. Sark-USA Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004) (“‘loss’ means any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made; h]owever, there is nothing to suggest that the “loss” or costs alleged can be unrelated to the computer”). Cf. *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>; *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1126-27 (W.D. Wash. 2000) (access and disclosure of trade secrets can constitute impairment of integrity under 18 U.S.C. § 1030(a)). For a detailed discussion of the case law on this issue across the spectrum of factual settings, see Robert D. Brownstone, 9 *Data Security & Privacy Law, Privacy Litig.* Ch. § 9:16 (West 2008).

¹⁵¹ *Brett Senior & Associates, P.C. v. Fitzgerald*, 2007 WL 2043377, *4 (E.D. Pa. July 13, 2007) (deletion of files did cause damage and thus violated section 1030(a)(5)(A)(i)).

¹⁵² Two Washington cases are most often cited for the proposition that damage under the act encompasses impairment of trade secrets: *Shurgard Storage Centers Inc. v. Safeguard Self Storage Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000); and *Pacific Aerospace & Electronic Inc. v. Taylor*, 295 F. Supp. 2d 1188 (E.D. Wash. 2003).

completeness or usability of data or information on a computer system."¹⁵³

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

Laws protecting union activity may hinder some types of electronic communications monitoring. In the private sector, traditionally mention of the National Labor Relations Act (NLRA) was more likely to conjure up images of steel mills than of e-mail servers. However, for some time, National Labor Relations Board (the Board) decisions have not hesitated to extend the protections of the NLRA to even white collar private sector employees’ use of e-mail.

In its 1997 *Timekeeping Systems, Inc.* decision,¹⁵⁴ the Board held that an employer violated the rights of its white-collar, non-unionized employees to engage in “protected concerted activity” when the employer terminated an employee for comments made on the company e-mail system.¹⁵⁵ The company’s Chief Operating Officer (COO) had sent an e-mail to employees soliciting their input on a proposed vacation and bonus plan. One employee had hit the “reply all” button, and in a “flippant and rather grating” e-mail pointed out (accurately) – to his manager and all recipients of the manager’s e-mail – several problems with the proposed changes.

The ALJ held that, notwithstanding its sarcastic tone, the e-mail was sent for the “purpose of mutual aid or protection” and was thus protected under Section 7 of the NLRA. The ALJ rejected the employer’s argument that the computer system had been disrupted by the e-mail, noting that the employer routinely allowed personal e-mail and telephone usage. Perhaps because it had used the e-mail system to solicit input from its employees about the vacation plan (and because it had apparently allowed personal use of its e-mail system), the employer in *Timekeeping Systems* did not press the point that it owned the e-mail system and was therefore entitled to restrict its use. The Board affirmed the ALJ’s order requiring reinstatement and back wages.

In an earlier case, the Board had held that a company could not prohibit the use of company computers to distribute union announcements when the company had (1) allowed

¹⁵³ *Garelli Wong & Associates, Inc. v. Nichols*, 551 F. Supp. 2d 704, 709 (N.D. Ill. 2008).

¹⁵⁴ *Timekeeping Systems, Inc.*, 323 NLRB No. 30 (1997).

¹⁵⁵ Section 7 of the NLRA protects the rights of employees to engage in “concerted activities for the purpose of . . . mutual aid or protection.” 29 U.S.C. § 157. Employers that interfere with these rights may violate Section 8(a)(1) of the NLRB. *See Id.* 29 U.S.C. § 158(a)(1). Employees enjoy Section 7 rights whether or not they work in a unionized enterprise.

personal use of the system and (2) encouraged members of a company-sponsored labor-management committee to use the e-mail system.¹⁵⁶

In the Spring of 2007, in the *Register-Guard* case, the NLRB heard oral argument on 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.¹⁵⁷

During 2007, while the Board's *Register-Guard* decision was pending, two pertinent decisions emerged, each coincidentally also involving a newspaper publisher. In March, in *Media Gen'l Operations, Inc. v. NLRB*, the Fourth Circuit affirmed an NLRB decision finding an unfair labor practice based on an employer's discriminatory enforcement of its e-mail policy's prohibition on non-business uses.¹⁵⁸ The employer had violated the NLRA by "ma[king] no attempt . . . to enforce the policy against any violations other than union messages[, given that t]he record contains numerous examples of messages unrelated to the work of the newspaper."¹⁵⁹ Then, in September, the NLRB rejected the validity of an employer's unilateral implementation of a revised e-mail policy where the employer had not first fulfilled its collective bargaining obligations.¹⁶⁰

At the very end of 2007, the NLRB issued its decision in *Register-Guard* by a 3-2 vote.¹⁶¹ Each of the majority and dissenting opinions contended that it was being consistent with the Fourth Circuit's *Media General* approach. 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

¹⁵⁶ See *E.I. du Pont de Nemours & Co.*, 311 NLRB No. 88 (1993). However, in analogous cases involving telephones, bulletin boards and videocassette players, the Board has upheld evenhanded restrictions on non-business use of company property to disseminate messages, even if they effectively bar the union from accessing those resources. See, e.g., *Mid-Mountain Foods, Inc.*, 332 NLRB No. 19 (2000) (employer did not violate NLRA when it did not allow union to show organizing video on VCR in employees' break room; no evidence that employees were allowed to play personal videos or that company had shown anti-union videos).

¹⁵⁷ *The Guard Publishing Company, d/b/a The Register-Guard*, Cases 36-CA-8743-1, et al. (Feb. 21, 2002), <<http://www.nlr.gov/nlr/about/foia/documents/J15-02sf.pdf>>.

¹⁵⁸ *Media Gen'l 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>>, cert. denied, 128 S. Ct. 492, 2007 WL 2383364 (U.S. Oct. 29, 2007).

¹⁵⁹ *Id.*

¹⁶⁰ *Calif. Newspapers Partnership d/b/a ANG Newspapers and N. Calif. Media Workers Guild/Typographical Union, Local #39521*, Case 32-CA-19276-1, 350 NLRB No. 89 (NLRB Sep. 10, 2007) <http://www.nlr.gov/shared_files/Board%20Decisions/350/v35089.pdf>.

¹⁶¹ *The Guard Publ'ng Co. d/b/a The Register-Guard and Eugene Newspaper Guild*, 351 NLRB No. 70 (12/16/07) <http://www.nlr.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.nlr.gov/shared_files/Press%20Releases/2007/R-2652.htm>.

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 is 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.

In other words, an apples-to-apples comparison of organization-to-organization is 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.¹⁶² 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.¹⁶³ Figuring prominently in the 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.¹⁶⁴

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.¹⁶⁵ 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*".¹⁶⁶ 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.

¹⁶² *Guard Publ'ng Co. d/b/a Register- Guard v. NLRB*, 571 F.3d 53 (D.C. Cir. July 7, 2009) <<http://pacer.cadc.uscourts.gov/common/opinions/200907/07-1528-1194980.pdf>>.

¹⁶³ *Id.* at 58.

¹⁶⁴ *Id.* at 60.

¹⁶⁵ *Id.* at 59.

¹⁶⁶ *Id.* at 60.

As noted in Section II(B)(2) above, the ultimate resolution of the *Register-Guard* issue set may have ripple effects in a variety of arenas.¹⁶⁷

In any event, 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

Employers may wish to prevent misconduct by regularly monitoring their computer systems and network resources.¹⁶⁸ However, to minimize the risk of employee privacy rights claims, an employer should implement an employee computer use policy that would enable it

¹⁶⁷ 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://www.nlr.gov/shared_files/GC%20Memo/2008/GC%2008-07%20Report%20on%20Case%20Development.pdf>. 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 28, 2008) <<http://pubs.bna.com/ip/bna/pvl.nsf/eh/a0b6n2q6y4>>; 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) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202421318139>>; see also uLoop informal settlement reflected at <http://mynlrb.nlr.gov/portal/nlr.pt/gateway/PTARGS_0_0_214_204_0_43/http%3B/s263492dc2ew05/icf/ECIS/CCBS/frnCissDisplayRecord.cfm?CN=21-CA-38223-001>; 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://pubs.bna.com/ip/bna/pvl.nsf/eh/a0b6k7p4e3>>.

¹⁶⁸ Lynn, Cecil, *Public ESI or Privileged Enforcement of Workplace Computer Privacy Policies*, BNA Privacy & Security Law Report (Nov, 17, 2008) (as does Robert Brownstone, this author calls Acceptable Use Policies “ ‘No Expectation of Privacy’ - ‘NEoP’ - policies”) <http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=11020416&vname=pvlrnotallissues&fn=11020416&jd=A0B7H5F8A2&split=0>; 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>>.

to monitor and search its computer network and systems at will.¹⁶⁹ See the ensuing Section V below for further discussion of the contents of such a computer use policy and related policies.

Most decisions regarding the interception of a private employee's e-mail has found that no intrusion into the employee's privacy occurred.¹⁷⁰

However, it is possible to construct some potentially viable privacy violations. For example, many states, including California and Michigan, recognize a right to privacy under state constitutional and/or common law.¹⁷¹ To prove a claim for the common law tort of invasion of privacy, an employee must establish that s/he had a reasonable expectation of privacy and that the employer's review of the private information would be highly offensive to a reasonable person.¹⁷²

In *Smyth v. Pillsbury Co.*,¹⁷³ plaintiff argued that his termination was wrongful because it was based on information obtained from e-mail messages in violation of his right of privacy. The court rejected this argument, stating, "Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."¹⁷⁴

It did not avail the employer that it had repeatedly told its employees that all workplace e-mail communications would be kept confidential and privileged. The court held that even if the employee's privacy right were violated, "the company's interest in preventing

¹⁶⁹ 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. See also SAMPLE ACKNOWLEDGMENT OF RECEIPT, at App. D-14.

¹⁷⁰ Talcott, Kelly D., "Cutting Out Privacy in the Office," N.Y.L.J. (12/19/07) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1198010085253>>; Bick, Jonathan, "E-Communications Policy: Getting It Right," E-Commerce Law & Strategy (Oct. 12, 2006) <www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1160557518711>.

¹⁷¹ See, e.g., *Miller v. National Broadcasting Co.*, 187 Cal. App. 3d 1463, 1482-84 (1986); *Baggs v. Eagle-Picher Industries, Inc.*, 957 F.2d 268 (6th Cir.), cert. denied, 506 U.S. 975 (1992). However, other states do not recognize a common law right to privacy. See generally Robert D. Brownstone, 9 *Data Security & Privacy Law*, Privacy Litig. Ch. § 9:83 (West 2008). ("[a]ll but a few states recognize at least one of the common law invasion-of-privacy torts, but not necessarily all four[; and s]everal states have also enacted statutes that codify and/or supplement the respective state's invasion-of-privacy common law").

¹⁷² Restatement (Second) of Torts § 625B.

¹⁷³ 914 F. Supp. 97 (E.D. Pa. 1996).

¹⁷⁴ *Id.* at 101.

inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.”¹⁷⁵

Several unpublished California cases have held similarly. For example, in *Bourke v. Nissan Motor Corp.*,¹⁷⁶ the court found that the employees had no reasonable expectation of privacy, and thus their privacy rights were not violated, because they had signed a form detailing that the use of the company computers was for business purposes only. In *Flanagan v. Epson*,¹⁷⁷ an employee brought a class action lawsuit alleging that Epson invaded the employees’ privacy by circumventing their passwords and reading their e-mail messages while fostering an atmosphere which led them to believe their messages were private. The *Flanagan* court refused to extend California’s right to privacy to employee e-mail, suggesting that such a determination should be left to the legislature. Likewise, in *Shoars v. Epson America*,¹⁷⁸ a \$75 million class action suit for invasion of privacy was dismissed, with the court observing that e-mail privacy is in the province of the legislature.

Courts have also found that employer monitoring and/or access of employee e-mail in a “personal folder” on a workplace computer is not an invasion of privacy.¹⁷⁹ In *Garrity v. John Hancock Mutual*,¹⁸⁰ the court rejected plaintiffs’ claims of a reasonable expectation of privacy based on the fact that they had personal passwords and e-mail folders. The court held that “[e]ven if plaintiffs had a reasonable expectation of privacy in their work e-mail, defendant’s legitimate business interest in protecting its employees from harassment in the workplace would likely trump plaintiffs’ privacy interests.”¹⁸¹

Courts have reached similar conclusions under the ECPA. In *Andersen Consulting LLP v. UOP*,¹⁸² Andersen was granted access to UOP’s internal e-mail system while providing consulting services. Andersen sued UOP for disclosure of its e-mail communications to a newspaper. The court dismissed, ruling that Andersen had to show that UOP had provided the electronic services to the public, not just to its employees and consultants.

¹⁷⁵ *Id.*

¹⁷⁶ No. B068705 (Cal. App. 2 Dist. July 26, 1993) (unpublished), *available at* <[http://www.louandy.com/CASES/Bourke v Nissan.html](http://www.louandy.com/CASES/Bourke_v_Nissan.html)>.

¹⁷⁷ *Flanagan v. Epson*, No. BC007036 (Cal. App. Dep’t. Super. Ct. 1990) (no published decision).

¹⁷⁸ *Shoars v. Epson America*, 1994 Cal. LEXIS 3670 (Cal. June 29, 1994).

¹⁷⁹ See *McLaren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103, 13 (TX 1999) (“the company’s interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh [plaintiff’s] claimed privacy interest in those communications”).

¹⁸⁰ *Garrity v. John Hancock Mutual Life Insurance Company*, 2002 U.S. Dist. LEXIS 8343; 146 Lab. Cas. (CCH) ¶ 59,541; 18 I.E.R. Cas. (BNA) 981 (D. Mass. May 7, 2002).

¹⁸¹ *Id.* at 6. *But see* the privilege issue in footnotes 96-98 and accompanying text above.

¹⁸² *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998).

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 computer was, until that time, [the employer]'s property."¹⁸³ Thus, the requisite element of a "highly offensive" intrusion was lacking as a matter of law.¹⁸⁴ 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.¹⁸⁵

The safest method to avoid liability under privacy laws is to achieve prior notice and consent.¹⁸⁶ 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.¹⁸⁷ See Section V below for further discussion of proactive policies.

III. INVESTIGATIONS AND BACKGROUND CHECKS

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

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. However, background checks 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.¹⁸⁸

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 municipal employers are unaware of the requirements of the . . . FCRA . . . , 15 U.S.C. §

¹⁸³ *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).

¹⁸⁴ *Id.* at 1204.

¹⁸⁵ *Id.*

¹⁸⁶ 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).

¹⁸⁷ 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.

¹⁸⁸ 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.

1681 et seq., which applies to hiring. In fact an even greater number of municipal employers fail to comply with the statute's provisions."¹⁸⁹

1. FACT Act Excludes Workplace Investigations From FCRA Requirements.

The 2003 amendments to the FCRA, titled "The Fair and Accurate Credit Transactions Act" (the "FACT Act")¹⁹⁰ made it significantly easier for employers to use outside investigators to conduct workplace investigations. The FACT Act specifically excludes from the definition of "consumer report" and "investigative report" any communications made to an employer in connection with an investigation of (1) suspected misconduct relating to employment; or (2) compliance with federal, state, or local laws and regulations or any preexisting written policies of the employer. Accordingly, employers may hire outside consultants, investigators, or law firms to investigate a variety of workplace issues without having to comply with the FCRA's notice and consent requirements.

Employers conducting investigations which the FACT Act otherwise excludes from the FCRA nonetheless must still provide the employee against whom an adverse employment action is taken a summary of the report and a summary of the employee's consumer rights.¹⁹¹

2. Non-FACT Act Investigations (Including Background Checks) Must Comply With FCRA Requirements

Employers using a consumer reporting agency to obtain a consumer report *not* related to workplace misconduct (such as a background check) must comply with the FCRA. The extent of the obligations FCRA imposes depends upon whether the information the CRA is requested to provide is classified as a "consumer report" or an "investigative consumer report." A "consumer report" is a report containing information bearing on an individual's "character, general reputation, personal characteristics, or mode of living." An "investigative consumer report" is a consumer report obtained through personal interviews. Most background checks fall into the consumer report category.

If an investigation is covered by the FCRA, the employer must notify the consumer (including applicants for employment) that it may obtain a consumer or investigative consumer report, and the employer must get the consumer's express written consent before obtaining a report.¹⁹²

¹⁸⁹ 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>> ("*Hiring Manual for Pa.*").

¹⁹⁰ Section 611 of the FACT Act relates to investigations.

¹⁹¹ 15 U.S.C. §§ 1681b(b)(3), 1681g(c)(3), 1681m(a). See generally FTC, *A Summary of Your Rights Under the Fair Credit Reporting Act* (July 8, 2004) <www.ftc.gov/os/2004/07/040709fcraappxf.pdf>. See also *Hiring Manual for Pa.*, supra note 189, at 109-122 (.pdf pp. 116-129).

¹⁹² See generally the sources cited at footnotes 189-91 above.

Under FCRA, employers have additional requirements if the report is an “investigative consumer report.” The employer must provide a second written notice to the consumer within three days of its request for an “investigative consumer report.” This notice must include a statement of the consumer’s right to request a complete and accurate disclosure of the nature and scope of the investigation and a summary of the consumer’s rights. If the consumer does request this additional disclosure, s/he must receive it within five days from the date the request was received or the date the company first requested the report, whichever is later. The company must also certify to the outside investigator that all required disclosures have been made.

In the event that an adverse decision is made based on either a consumer report or an investigative consumer report, the company must provide the consumer with oral, written, or electronic notice of the adverse employment action and the name, address, and telephone number of the consumer reporting agency making the report, including a toll-free number if the reporting agency compiles and maintains files on consumers on a nationwide basis. The company must also provide a statement that the consumer reporting agency did not make the adverse employment decision and that the CRA is unable to provide the specific reasons why the adverse action was taken. (See **Attachment 4**: “FCRA Disclosure For Adverse Action Based On Non-FACT Act Investigation”). In addition, the employer must provide the employee a copy of the report with no redactions aside from sources of information, and a copy of his or her consumer rights.

3. Outside Investigations Must Comply with State Regulatory Schemes Such as California’s ICRAA

The California Investigative Consumer Reporting Agencies Act (ICRAA) regulates investigations in California. Similar to the FCRA, the ICRAA covers “investigative consumer reports” including any record of an individual’s “character, general reputation, personal characteristics or mode of living.” This could include reference checks, criminal background checks, and investigations of employee harassment and misconduct, as discussed more fully below.

ICRAA was amended in 2002 to add a key clarification that employers conducting investigations *without* the assistance of a consumer reporting agency are NOT required to comply with ICRAA’s procedural requirements. There is only one exception to this new rule: If the information collected internally is a “matter of public record,” it must nonetheless be disclosed to applicants and employees within seven days. However, if the employer obtains a public record for the purpose of conducting an investigation for suspicion of wrongdoing or misconduct by the subject of the investigation, the employer may withhold the information until the completion of the investigation. Upon completion, the employer shall provide a copy of the public record to the consumer, unless the consumer waived his or her rights.¹⁹³

The 2002 amendments also changed California law with respect to investigations conducted with the assistance of a “consumer reporting agency,” as follows:

- Employers must provide notice and obtain consent every time they seek an investigative consumer report from an outside entity on an applicant or employee for employment purposes (defined as for the purpose of “evaluating a consumer for employment, promotion, reassignment, or

¹⁹³ Cal. Civ. Code §1786.53.

retention as an employee”¹⁹⁴), other than suspicion of wrongdoing or misconduct by the subject of the investigation.

- Employers are no longer required to provide a copy of the consumer report to applicants or employees, except where the employee has specifically requested a copy by checking a box on a form, which must be provided by the employer, on the notice and authorization form. If the employee does request a copy, the employer must send a copy of the report to the employee within three business days of the date the employer received the report.
- If an adverse action is taken as a result of the report, the employer must advise the applicant that the adverse action is being taken and supply the contact information of the consumer reporting agency used. Once again, no such requirement applies if the investigation involves suspected misconduct or wrongdoing.

It remains unclear whether the California courts will interpret ICRAA to mean that outside law firms conducting corporate investigations are de facto corporate employees not triggering ICRAA’s consumer reporting obligations.

B. Legality and Advisability of Following the Internet Trail

Much has been written recently about the “brave new world of Web 2.0 and the quandary it creates for employers considering hiring a given applicant.”¹⁹⁵ 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.¹⁹⁶
- An employer may lawfully search/Google as to an applicant.¹⁹⁷

¹⁹⁴ Cal. Civ. Code § 1786.2.

¹⁹⁵ See, e.g., Vickie L. Wallen and Brian Flock, *Social Networking Sites Pose Risk For Employers*, Law 360 (Jan. 28, 2009) <http://www.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) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202426302782>> (discussing inconclusive decision in *Corman v. UCG*, 369 F. Supp. 2d 923 (N.D. Ohio 2005) <<https://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>>.

¹⁹⁶ See generally 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>> (citing, *inter alia*, *Duran v. Detroit News, Inc.*, 200 Mich. App. 622, 504 N.W. 2d 715, 21 Media L. Rep. 1891 (Mich. App. 1993), *appeal denied*, 444 Mich. 944, 512 N.W.2d 846 (Mich. 1994)).

¹⁹⁷ *Mullins v. Dep’t of Commerce*, No. 06-3284, 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>>.

- 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,¹⁹⁸ 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.¹⁹⁹
 - 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 pitfalls of trying to parse – 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.²⁰⁰ On the other hand, as at least one employer has publicly announced it is doing, an organization can decide to avoid web research altogether.²⁰¹

When the prospective employer is a public entity, even greater care may be necessary.²⁰² Last year, 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.*,²⁰³ 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

¹⁹⁸ See Section IV(D) below.

¹⁹⁹ For a stark example, see Molly DiBianca, *Twitter Saves Cisco a Bundle of Money*, Del. Emp. Law Blog (Mar. 30, 2009) <http://www.delawareemploymentlawblog.com/2009/03/twitter_saves_cisco_a_bundle_o.html>.

²⁰⁰ 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>>.

²⁰¹ 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>>.

²⁰² See Fenwick & West, *Unnecessarily Broad Background Checks Halted As an Invasion of Privacy*, Emp. Brief (Feb. 8, 2008) (discussing the now-vacated *Nelson I* decision) <<http://www.fenwick.com/publications/6.5.4.asp?mid=31#nb>>, from which the ensuing discussion is adapted.

²⁰³ *Nelson v. NASA*, 530 F.3d 865 (9th Cir. 2008) (*Nelson II*) <<http://www.ca9.uscourts.gov/datastore/opinions/2008/06/19/0756424.pdf>>.

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.

Although the *Nelson* ruling was limited to background searches conducted by a government agency, private sector employers should remain mindful of the privacy protections offered by federal and state law and carefully consider the appropriate breadth of proposed background checks.

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. State constitutional or common law privacy theories typically require balancing employers' interests with employee expectations of privacy. In *K-Mart Corp. Store No. 7441 v. Trotti*,²⁰⁴ a Texas court found that a search of a company-owned locker violated an employee's right to privacy. In that case, the employee placed her purse in a locker and secured the door with her own lock. When she returned to the locker during her afternoon break, she discovered the lock hanging open and her purse in disorder. The manager had opened the lock because of a suspicion that an unidentified employee had stolen a watch. The employee filed a lawsuit for invasion of privacy.

The Texas court reasoned that the company policy allowing employees to purchase and use their own locks on lockers, without requiring the employees to give the combination or key to the employer, justified the employee's expectation that the locker and its contents would be free from intrusion and interference. Moreover, the covert nature of the intrusion, without permission from the employee, contributed to the damages the employee suffered.

In *Gossmeyer v. McDonald*, the Seventh Circuit adopted a test of "reasonableness," and held that an employer's unannounced search of the desk and filing cabinet of a child-protection investigator was reasonable in light of an anonymous tip that the investigator kept pornography in the office.²⁰⁵ The court concluded that the file cabinet, even though purchased by the plaintiff, was primarily for workplace materials.²⁰⁶

As with electronic monitoring, setting employee expectations is one of the most effective ways to avoid workplace search liability. If an employer anticipates needing to search its employees' work areas, it should consider including written notice specifying which

²⁰⁴ *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632 (Ct. App. Texas 1984).

²⁰⁵ *Gossmeyer v. McDonald*, 128 F.3d 481 (7th Cir. 1997).

²⁰⁶ *Id.*

areas are subject to search, the triggering circumstances and the protocols that will be used. While such policies may not always be dispositive in a court's determination as to whether employees have a reasonable expectation of privacy, employers will increase their chances of prevailing if they can demonstrate that any search was conducted in accordance with written policies and that employees were made aware of the policies.²⁰⁷

As to public employers, as discussed above regarding *Quon*,²⁰⁸ the Fourth Amendment may be implicated by physical searches as well as by searches for electronically stored information. Recently, 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.²⁰⁹ Significantly, however, the same decision denied summary judgment on her Fourth Amendment claim.²¹⁰

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*,²¹¹ the Ninth Circuit upheld a random search of an employee's backpack by a security guard in large part because the employee was aware of the employer's policy that it would conduct random searches.²¹² 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."²¹³

²⁰⁷ See e.g., *McDowell v. Frank*, 1992 U.S. Dist. LEXIS 16863 (D. Cal. 1992) (employer defeated employee's claims for invasion of privacy because employer reserved the right to search lockers).

²⁰⁸ See notes 111-116 and accompanying text above, including as to the conflicting standards debated by the Ninth Circuit.

²⁰⁹ *Brown-Criscuolo v. Wolfe*, --- F.Supp.2d ----, 2009 WL 585910 (D. Conn. Mar. 9, 2009) <<https://ecf.ctd.uscourts.gov/doc1/04102051731>>.

²¹⁰ *Id.* But see *U.S. v. Larson*, 66 M.J. 212 (U.S. Armed Forces Apr. 25, 2008) (distinguishing the *Long* case discussed in footnote 97 above) <<http://www.armfor.uscourts.gov/opinions/2008Term/07-0263.pdf>>., *cert. denied*, 129 S. Ct. 267, 172 L.Ed.2d 148 (U.S. Oct. 06, 2008)

²¹¹ *United States v. Gonzalez*, 300 F.3d 1048 (9th Cir. 2002).

²¹² *Id.* at 1055.

²¹³ *Id.*

B. Video Surveillance

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.²¹⁴ At least one federal circuit has held that the ECPA does not encompass video surveillance where the recording does not capture audio.²¹⁵

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. For instance, the California Supreme Court held that a journalist's use of a hidden camera in a workplace can be an invasion of privacy, upholding a \$1.2 million jury verdict against ABC News over a story about telephone psychics.²¹⁶ Plaintiff, Sanders, sued a someone he thought was a co-worker. The defendant was actually a reporter who, while employed by ABC, had obtained employment as a "telepsychic" and wore a small video camera and covertly videotaped conversations in the workplace. Plaintiff sued for invasion of privacy by intrusion.²¹⁷

In *Sanders*, Plaintiff ultimately won his case against the reporter and ABC. At trial, a jury found for Plaintiff. On appeal, the intermediate appellate court reversed on the ground that plaintiff could have no reasonable expectation of privacy in his workplace conversations which could be overheard by others in a shared office space. However, the California Supreme Court then reversed the appellate court, concluding that in an office or other workplace to which the general public did not have unfettered access, employees enjoyed a limited, but legitimate, expectation that their conversations and other interactions would not be secretly videotaped, even though those conversations may not have been completely private.²¹⁸ It explained that "in the workplace, as elsewhere, the reasonableness of a person's expectations of visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion."²¹⁹

²¹⁴ 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 Telephone Co.*, 110 F3d 174 (1st Cir. 1997).

²¹⁵ *Thompson v. Johnson County Community College*, 1997 U.S. App. LEXIS 5832 (10th Cir. 1997) (unpublished opinion).

²¹⁶ *Sanders v. American Broadcasting Companies*, 20 Cal. 4th 907 (1999).

²¹⁷ *Id.* at 910.

²¹⁸ *Id.* at 917.

²¹⁹ *Id.* at 924.

Just a few weeks ago, in the California Supreme Court revisited in great detail the issues it had addressed in *Sanders*.²²⁰ This new 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.²²¹

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.²²² 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."²²³ 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.

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."²²⁴ Defendant Director "did not expect or intend to catch plaintiffs on tape."²²⁵ Based in large part on those facts, the California Supreme Court agreed with the trial court that summary judgment was

²²⁰ *Hernandez v. Hillsides, Inc.*, ___ Cal. Rptr. 3d ___, 2009 WL 2356904 (Cal. Aug. 3, 2009) <www.courtinfo.ca.gov/opinions/documents/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/ca/PubArticleFriendlyCA.jsp?id=1202432750574>>; 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>

²²¹ *Id.* at *8.

²²² *Id.* at *14, *19.

²²³ *Id.* at *1.

²²⁴ *Id.*

²²⁵ *Id.*

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. States such as California have statutes outright prohibiting videotaping in certain locations.²²⁶ 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.

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.²²⁷ Moreover, video surveillance may be a mandatory bargaining subject in union shops.²²⁸

C. GPS Tracking – including RFID and GPS

Some employers have adopted emerging 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 and can range 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.

²²⁶ 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>.

²²⁷ See *Clement v. ITT Sheraton Boston Corp.*, 1993 Mass. Super. LEXIS 314 (1998) (discussing other legal issues prior to settlement).

²²⁸ See generally Norman Brand (editor-in-chief), *Discipline and Discharge in Arbitration*, Ch. 13, § XI(B)(2), *External Law – Monitoring – Surveillance*, (BNA 2d ed. 2008) <http://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)(l)(i) (*Evidence – Arbitrator Consultation of Experts – Search of an Employee’s Person or Property – Surveillance of Employees* (BNA 2003 & Supp. 2008) <http://storefront.bnabooks.com/epages/bnastore.sf/en_US/?ObjectPath=/Shops/bnastore/Products/9592>.

Employers who currently use GPS technology are in the minority, with only 3 percent using GPS to monitor cell phones,²²⁹ 8 percent using GPS to track company vehicles,²³⁰ and less than 1% percent using GPS to monitor employee ID/Smartcards.²³¹

The majority of companies using RFID employ Smartcard technology to control physical security and access to buildings and data centers.²³² 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.²³³

While use of these technologies has not yet been widely adopted, the basic infrastructure is in place. The Federal Communications Commission ("FCC") imposed a December 31, 2002 deadline on mobile telephone service providers to update product lines to include only phones capable of pinpointing a user's location.²³⁴ Thus, companies can now track the location of most employees who carry modern mobile telephones.

A couple years ago, CityWachter.com, an Ohio surveillance company, spurred on the RFID controversy when it announced that it embedded RFID tags in two of its employees.²³⁵ RFID chips are used increasingly to track everything from product shipment to pets. VeriChip, the company that makes the devices, said the implants were created primarily for medical purposes.

RFID and GPS raise somewhat unique monitoring issues as they are more likely than other technologies to capture off-duty conduct. For example, the owner of a car alarm installation company terminated one of his employees after learning through use of a wireless tracking device that the employee's vehicle had been parked at a strip club.²³⁶

Even where employers have a legitimate reason to use such technologies, there is a risk of misinterpreting GPS information. One employer terminated a delivery driver when it

²²⁹ 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>>.

²³⁰ *Id.*

²³¹ *Id.*

²³² *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>>.

²³³ 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>.

²³⁴ 47 CFR § 20.18(g)(1)(iv).

²³⁵ Richard Waters, *US Group Implants Tags in Workers*, Financial Times, Feb. 12, 2006.

²³⁶ Simon Romero, *Location Devices Use Rises, Prompting Privacy Concerns*, New York Times, March 4, 2001.

discovered through GPS that the employee was not taking the most direct routes.²³⁷ The employer refused to reconsider its decision to terminate despite the employee's protestation that he only took the indirect routes to avoid tolls.²³⁸

One study by the Rand Corporation uncovered other potentially troubling uses of RFID.²³⁹ Although it only sampled a handful of employers, the study's authors found that most of the companies using RFID access control systems linked such systems to other personally identifiable information.²⁴⁰ One employer even linked its RFID access badges to employee medical information.²⁴¹ The study also revealed other potential problems including the fact that most companies surveyed lacked a written policy on RFID use. The study also found that most companies surveyed retained the RFID data indefinitely and that the companies lacked any external auditing process for ensuring that such data are accurate.²⁴²

In contrast to the present technological viability for RFID and GPS monitoring, biometric identification tools are not yet viable, at least on a widespread level, according to a presentation by Richard Carter of the American Association of Motor Vehicle Administrators ("AAMVA").²⁴³ AAMVA studied whether the use of biometric identifiers would help create better identification cards, and the association concluded it would not recommend the use of any biometrics on the interstate level.²⁴⁴ Carter noted that the representations in movies and television of biometric (such as facial recognition) as being highly advanced and effective are simply not true.²⁴⁵ Melissa Ngo, staff counsel at the Electronic Information Privacy Center, said that many biometric tools, and in particular facial recognition technology, have high rates of unreliability.²⁴⁶ "Biometrics has been grossly oversold by government and industry for many years," according to Frank Moss, deputy assistant secretary at the State Department.²⁴⁷

²³⁷ *In re Superior Products*, 116 Lab. Arb. Rep. (BNA) 1623.

²³⁸ *Id.*

²³⁹ Balkovich, Bikson and Bitko, *9 to 5: Do You Know if Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace* (2005).

²⁴⁰ *Id.* at 15.

²⁴¹ *Id.*

²⁴² *Id.*

²⁴³ Donald Aplin, "Widespread Use of Biometric Identity Tools Not Yet Viable, Unlikely in Real ID Act Rule," BNA Privacy & Security Law Report, March 13, 2006.

²⁴⁴ *Id.*

²⁴⁵ *Id.*

²⁴⁶ *Id.*

²⁴⁷ *Id.*

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 statutory protection for employees’ off-duty conduct, and that number increases when one includes states that regulate this area through common law privacy protections.²⁴⁸

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

Employers have a clear interest in preventing their employees from engaging in direct competition during their employment; however, an employer’s ability to prohibit all moonlighting varies based on several factors, including the employee’s position and whether the moonlighting activity is truly competitive. Thus for example, employers may usually restrict someone employed as an engineer from performing engineering work for a direct competitor. The California labor code speaks to this issue directly: “An employee who has any business to transact on his own account, similar to that entrusted to him by his employer, shall always give preference to the business of the employer.”²⁴⁹

In *Stokes v. Dole Nut Co.*, two managerial-level employees worked surreptitiously making preparations to establish a business in direct competition with Dole.²⁵⁰ Upon finding

²⁴⁸ See, e.g., Molly DiBianca, *Terminating Employees for Off-Duty Conduct*, Del. Emp. Law Blog (Oct. 20, 2008) <http://www.delawareemploymentlawblog.com/2008/10/terminating_employees_for_offd_3.html>.

²⁴⁹ California Labor Code § 2863.

²⁵⁰ *Stokes v. Dole Nut Co.*, 41 Cal. App. 4th 285 (1995).

that they were engaged in this practice, Dole terminated both employees. The employees subsequently sued Dole for breach of implied and express contract of continued employment and breach of the implied covenant of good faith and fair dealing.

At trial, the employees asserted that mere preparations to compete, whether or not disclosed, could not be cause for termination. However, the court emphasized that the employees were at a managerial and supervisory level, and had access to confidential company information. In addition, it was revealed over the course of the litigation that the employees planned to rely on key contacts they had made through their Dole employment.

In reaching its decision, the court emphasized that an employer need not wait until the employee commits a tortious act to terminate his employment. "The point at which an employee's outside activities warrant termination is dependent upon the particular circumstances of the case."²⁵¹ In this case, the court found that the employees' "outside activities had progressed to the point that conflicts of interest compromised Dole's right to their undivided loyalties."²⁵²

2. Substance Use

Employers clearly have a legitimate interest in preventing their employees from arriving at work under the influence of illegal narcotics or alcohol.²⁵³

Even where an employer can show that an employee has used illegal narcotics, the employer often needs to show that the drug use impacts the employee's ability to perform. For example, in *Baldor Elec. Co. v. Reasoner*,²⁵⁴ the employer imposed a policy requiring employees to submit to drug testing whenever they suffer a work-related injury resulting in medical treatment and further provided that a positive test result would be grounds for discipline, up to and including termination, even for the first offense.²⁵⁵ After suffering an on-the-job injury, the employee was required to undergo a urine test, which came back positive indicating a low-level presence of marijuana.²⁵⁶ The employee was discharged despite working for the employer for 17 years without a prior incident of any kind.

When the employee appealed a denial of unemployment benefits, the reviewing court held that the relevant inquiry was whether the employee's off-duty conduct affected her ability to fulfill her responsibilities to the employer. The court concluded that the employer failed to meet its burden of proving that the employee was terminated for misconduct because it failed to offer expert testimony or any other explanation demonstrating that such a low level of the drug in any way impaired the employee's ability to meet her on-the-job

²⁵¹ *Id.* at 296.

²⁵² *Id.*

²⁵³ See generally Nancy N. Delogu, *Substance Abuse; Trends in Employee Drug Testing*, Cal. Lawyer (Mar. 2007) <<http://www.callawyer.com/story.cfm?pubdt=NaN&eid=884313&evid=1>>.

²⁵⁴ *Baldor Elec. Co. v. Reasoner*, 66 S.W.3d 130 (Mo. Ct. App. 2001).

²⁵⁵ *Id.* at 132.

²⁵⁶ *Id.*

responsibilities to the employer.²⁵⁷ The court explained that the employer could not supplant the statutory requirement of proving misconduct connected with work and reduce its statutory unemployment insurance responsibilities through the promulgation of its own work rules, especially when such rules purported to regulate the off-duty conduct of its employees.²⁵⁸

Some employers seek to reach beyond activity that directly relates to on-duty conduct. For example, in the face of rising health care costs, one intrepid employer made news a few years ago, when it sought to impose a company-wide smoking ban. Weyco Inc., an employee-benefits administrator in Michigan, made national news when it imposed a company-wide ban, which was phased in over two years.²⁵⁹ In 2003, Weyco quit hiring tobacco users and forbade its staff from smoking on the premises. Starting in 2004, the firm added a tobacco "assessment" of \$50 a month per worker who smoked and didn't go to a cessation class. Weyco had given its employees a 15-month advance notice that those who still smoked on or off the company's watch by January 2005 would be terminated, according to the company's founder and CEO. Subsequently Weyco's policy became even stricter, "expand[ing] the policy to spouses of its 175 employees. If the spouses test[ed] positive for nicotine in monthly tests, the employee [had to] pay an \$80 monthly fee until the spouse t[ook] a smoking cessation class and test[ed] nicotine-free."²⁶⁰

Employers wishing to implement such bans should first consult the laws of the jurisdiction in which they operate: at least 17 states have statutes expressly protecting employees' right to use tobacco products away from work.²⁶¹ However, some of these state statutes contain exceptions where the employer can show that the smoking ban reasonably relates to a bona fide occupational requirement. Thus, in *Wood v. South Dakota Cement Plant*,²⁶² a company that required employees to refrain from smoking because of on-the-job exposure to dust successfully defended itself for terminating an employee who repeatedly tested positive for nicotine. The employee filed suit, claiming he was terminated in violation of South Dakota's law protecting employees' right to smoke while off-duty.²⁶³ The court

²⁵⁷ *Id.* at 134.

²⁵⁸ *Id.*

²⁵⁹ Mark Rowh, *Policing Lifestyles*, HR Executive Online (July 1, 2005) ("[m]ore employers are looking for ways to encourage workers away from unhealthy habits; but at what point does encouragement cross the privacy line?") <<http://www.hreonline.com/HRE/printstory.jsp?storyId=4223279>>.

²⁶⁰ Amy Joyce, *So Much for 'Personal' Habits*, Wash. Post (Oct. 15, 2006) <www.washingtonpost.com/wp-dyn/content/article/2006/10/14/AR2006101400105_pf.html>.

²⁶¹ See, e.g., the following states' statutes prohibiting employer interference with employees' use of tobacco products outside of work: Ariz. Rev. Stat. 36-601.02(f); D.C. Code Ann. 7-1703.03; Ind. Code Ann. 22-5-4-1; Ky. Rev. Stat. Ann. 344.040(3); La. Rev. Stat. Ann. 23:966; Me. Rev. Stat. Ann. tit. 26, 597; Miss. Code Ann. 71-7-33; N.H. Rev. Stat. Ann. 275:37-a; N.J. Stat. Ann. 34:6B-1; N.M. Stat. Ann. 50-11-3; Okla. Stat. tit. 40, 500; Or. Rev. Stat. 659A.315; R.I. Gen. Laws 23-20.7.1-1(a); S.C. Code Ann. 41-1-85; S.D. Codified Laws 60-4-11; Va. Code Ann. 15.2-1504; W. Va. Code 21-3-19; Wyo. Stat. Ann. 27-9-105(a)(iv).

²⁶² *Wood v. South Dakota Cement Plant*, 1999 SD 8 (S.D. 1999).

²⁶³ *Id.*

denied plaintiff's claim, holding that the employer did not violate the South Dakota law because the smoking restriction related to a bona fide occupational requirement and was reasonably and rationally related to the employment activities and responsibilities.²⁶⁴

Note also that the rules may very well be different with respect to public entity employers, as to which a greater justification may be required under federal and/or state constitutional law. Last year, the Ninth Circuit Court of Appeals that a city in Oregon could not rescind an offer of employment to someone who had declined to be tested under the City's pre-employment drug and alcohol screening policy.²⁶⁵ There, the appellate court affirmed a summary judgment in the applicant's favor as well as a declaratory judgment that the City's policy was facially unconstitutional because unsupported by any special need outweighing the reasonable expectation of privacy.²⁶⁶ The court opined that, in contrast to the pertinent job as a library page, drug testing could be required for some city jobs requiring, for example, operating machinery or working directly with children.²⁶⁷

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, policies restricting office romance implemented in an effort to prevent sexual harassment claims have been upheld. For example, in *Sanguinetti v. UPS*,²⁶⁸ the employer had a no-dating rule that prohibited managers from having sexual relationships with other employees. UPS's rule stated:

Relationships between employees other than professional relationships, can lead to detrimental effects in the workplace with customers; affect the respect, dignity and rights of co-workers; and may incur liability on the part of our company. Unprofessional relationships potentially expose participants and our company to allegations of sexual harassment, favoritism, conflict of interest and breach of confidentiality. Each of us has the responsibility for creating and maintaining professional relationships.²⁶⁹

²⁶⁴ *Id.*

²⁶⁵ *Lanier v. City of Woodburn*, 518 F.3d 1147, 1149, 1152 (9th Cir. 2008) (city's action unconstitutional under Fourth Amendment as well as Art. I § 9 of the Oregon Constitution) <<http://www.ca9.uscourts.gov/datastore/opinions/2008/03/12/0635262.pdf>>.

²⁶⁶ *Id.* at 1150-52.

²⁶⁷ *Id.* at 1151-52.

²⁶⁸ *Sanguinetti v. UPS*, 114 F. Supp. 2d 1313 (D. Fla. 2000).

²⁶⁹ *Id.* at 1315.

The UPS Policy Book also stated that UPS managers had “the responsibility to avoid any relationships that may result in actual or perceived favoritism.”²⁷⁰

A dispute implicating the lawfulness of UPS’s policy arose when a recently-promoted manager started a romantic relationship with an hourly employee. When the manager attempted to end the relationship, the hourly employee allegedly came to his house and threatened to report him.²⁷¹ The manager complained that the hourly employee was harassing him. Instead of acting on the sexual harassment claim, UPS terminated the manager for violating the company’s prohibition on dating coworkers.²⁷² The manager sued for wrongful termination. While the court did not directly address the legitimacy of UPS’s dating prohibition, it concluded that the manager could not go forward with his wrongful termination claim, thereby implicitly finding that UPS’s policy was a lawful restriction on off-duty conduct.²⁷³

Even New York, which has one of the more sweeping statutes protecting lawful off-duty conduct, has recognized that employer prohibitions on dating relationships between coworkers may be lawful. New York’s ambiguously worded statute protects employees’ “legal recreational activities”²⁷⁴ and provides employees with a private right of action for equitable relief and damages.²⁷⁵ Not surprisingly, litigation arose relating to whether personal intimate relationships fall within the protection of “legal recreational activities.” In *McCavitt v. Swiss Reinsurance America Corp.*,²⁷⁶ an employee alleged that he was passed over for a promotion and then terminated because of his romantic relationship with another officer of the company. McCavitt was terminated despite the fact that the employer did not have a written non-fraternization policy, and the relationship allegedly did not have any “repercussions whatsoever for the professional responsibilities” of the terminated employee. Nonetheless, the court concluded that romantic relationships are not “legal recreational activities” protected by the New York statute.

More recently, namely a year ago, in another UPS case, 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*,²⁷⁷

²⁷⁰ *Id.*

²⁷¹ *Id.*

²⁷² *Id.*

²⁷³ *Id.*

²⁷⁴ N.Y. Lab. Law 201-d(2).

²⁷⁵ NY CLS Labor § 201-d(7)(b): “In addition to any other penalties or actions otherwise applicable pursuant to this chapter, where a violation of this section is alleged to have occurred, an aggrieved individual may commence an action for equitable relief and damages.”

²⁷⁶ *McCavitt v. Swiss Reinsurance America Corp.*, 237 F.3d 166 (2d Cir. 2001).

²⁷⁷ *Ellis v. UPS*, 523 F.3d 823 (7th Cir. 2008) <<http://www.ca7.uscourts.gov/tmp/N31FG5A8.pdf>>. See generally Fenwick & West, *Manager Fired For Violating Policy, not Interracial Relationship*, Emp. Brief (May 15, 2008) <<http://www.fenwick.com/publications/6.5.4.asp?mid=34#manager>>, from which the ensuing discussion was adapted.

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.²⁷⁸ 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, late last year, 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.²⁷⁹

4. Arrests and Convictions

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 Act²⁸⁰ prohibits employers from discriminating against an

²⁷⁸ *Lynn v. Wal-Mart Stores, Inc.*, 2008 WL 725604 (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) <http://www.delawareemploymentlawblog.com/2008/05/employers_private_eyes_are_wat.html?action=print>.

²⁷⁹ *Lehto v. Board of Education of the Caesar Rodney School District*, 962 A.2d 222 (Del. 2008) <[http://courts.state.de.us/opinions/\(a4sdyjni0why1t55z0gv2v45\)/download.aspx?ID=114560](http://courts.state.de.us/opinions/(a4sdyjni0why1t55z0gv2v45)/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>.

²⁸⁰ Wis. Stat. § 111.321.

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."²⁸¹

Late last year, Starbucks defeated a class action arising out of the criminal background question in its job application.²⁸² 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.²⁸³ 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.²⁸⁴ 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.

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. 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 15 months:

²⁸¹ Wis. Stat. 111.335(1)(b).

²⁸² 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>>.

²⁸³ *Starbucks Corp. v. Superior Court*, 168 Cal. App. 4th 1436, 86 Cal. Rptr. 3d 482 (Cal. App. 4 Dist. 2008) <<http://www.courtinfo.ca.gov/opinions/archive/G039700.PDF>>.

²⁸⁴ *Id.*

- 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;”²⁸⁵
- a negatively evaluated Pennsylvania high school student-teacher, whose non-receipt of a teaching credential has been upheld in light of her posting a photo of herself – captioned the “Drunken Pirate” – on her MySpace page;²⁸⁶
- a suspended North Carolina school teacher, who is also facing possible termination, based on her posting racially derogatory comments on her own Facebook page;²⁸⁷
- 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;²⁸⁸
- an Iowa community college president, who resigned after a newspaper reported “that 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.”²⁸⁹

²⁸⁵ *Dible v. City of Chandler*, 515 F.3d 918, 924 (9th Cir. 2008) <www.ca9.uscourts.gov/datastore/opinions/2008/01/31/0516577.pdf> (discussing *City of San Diego v. Roe*, 543 U.S. 77, 125 S. Ct. 521, 160 L.Ed.2d 410 (2004) <<http://laws.findlaw.com/us/000/03-1669.html>>). See generally D. Gregory Valenza, *Overexposed Employees*, Daily J. (Apr. 17, 2009) <<http://shawvalenza.com/publications.php?id=223>>.

²⁸⁶ *Snyder v. Millersville University*, No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008) <<https://ecf.paed.uscourts.gov/doc1/15304792325>>. See generally 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) <<http://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>>.

²⁸⁷ 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>.

²⁸⁸ *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>.

²⁸⁹ 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>.

- a fired Swiss insurance worker, whose at-home Facebook activity belied her prior contention that, when out on sick leave, she could not use a computer screen;²⁹⁰
- 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;²⁹¹ and
- a former high school student whose privacy causes of action were dismissed against the principal of her alma mater, who had forwarded to the press a negative ode the student had previously published on her own MySpace page.²⁹²

V. IMPLEMENTING LEGALLY-COMPLIANT AND DEFENSIBLE POLICIES

A. Introduction to Compliance

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

The “Three E’s” theory was alluded to at the end of Section I(A) above and as cited in Section V(D) below: 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. A 2006 survey concluded that 76% of employers have implemented a written e-mail policy governing use and content, 55% monitor employee outgoing and incoming e-mail, and 76% monitor employee Internet connections.²⁹³

Moreover, only 34% have an e-mail retention policy, in spite of the fact that 34% of employees do not know the difference between business-critical e-mail that must be saved and insignificant messages that may be purged.²⁹⁴ As for governmental entities, there is a heightened need for an e-mail (and overall) retention policy – given the need for a compliance approach as to various FOIA-type open-government/public-records/sunshine

²⁹⁰ Emma Thomasson, Facebook surfing while sick costs Swiss woman job, Reuters (Apr. 24, 2009) <http://www.washingtonpost.com/wp-dyn/content/article/2009/04/24/AR2009042402019_pf.html>.

²⁹¹ 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>>.

²⁹² *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 91 Cal. Rptr. 3d 858 (Cal. App. 5 Dist. Apr. 2, 2009) <<http://www.courtinfo.ca.gov/opinions/documents/F054138.PDF>>. See also Valenza supra note 285.

²⁹³ See American Management Association and ePolicy Institute, *2006 Workplace E-Mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-Mail, IM & Blog Violators* <http://www.amanet.org/press/amanews/2006/blogs_2006.htm/>.

²⁹⁴ *Id.*

laws.²⁹⁵ and as to other, more concrete legally imposed retention requirements.²⁹⁶ Similarly, only 31% of surveyed employers have adopted an Instant Messaging ("IM") policy, and only 13% retain and archive, business record IM.²⁹⁷

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

Prophylactic agreements and policies can cut off future protracted litigation disputes.²⁹⁸ 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

²⁹⁵ See, e.g., California Public Records Act (CPRA), Gov't Code, § 6250, *et seq.*, as summarized in detail at <http://www.ag.ca.gov/publications/summary_public_records_act.pdf>; D.C. Government Administrative, *E-mail Retention Policy*, Mayor's Order 2007-157 <http://octo.dc.gov/octo/frames.asp?doc=/octo/lib/octo/information/pdf/2007-157_Email_Retention_Policy.pdf>; Georgia Open Records Act ("GORA"), OCGA § 50-18-70, *et seq.*; Idaho Public Records Law, I.C. §§ 9-301-9-350; Wisconsin Public Records Law, Wis. Stat. § 19.31, *et seq.* (2003–04). Under those respective laws, e-mail disclosures and other electronic-information disputes have come to the fore this past year in many situations, including the following ones: *LAUSD v. Superior Court (City of Long Beach)*, 151 Cal. App. 4th 759, 60 Cal. Rptr. 3d 445 (Cal. App. 2 Dist. 2007) (one public agency can seek disclosure of records from another public agency) <<http://caselaw.findlaw.com/data2/californiastatecases/B193566.PDF>>; Yolanda Woodlee, *City E-Mails to Be Purged After 6 Months*, Wash. Post (Aug. 2, 2007) (discussing e-mail retention approaches in Akron, Cincinnati, D.C. and Philadelphia) <http://www.washingtonpost.com/wp-dyn/content/article/2007/08/02/AR2007080202454_pf.html>; *Georgia Dept. of Agriculture v. Griffin Indus.*, 284 Ga. App. 259, 644 S.E. 2d 286 (2007) (addressing whether state agency had to restore email from back-up tapes to respond to open records law request); *Cowles Pub. Co. v. Kootenai County Bd. of County Com'rs*, 144 Idaho 259, 159 P.3d 896 (2007) (e-mails between public employees were public records and, due to signed County e-mail policy, were not protected by legitimate privacy expectation) <<http://www.isc.idaho.gov/opinions/cowles14.pdf>>; *Wiredata, Inc. v. Village of Sussex*, 298 Wis. 2d 743, 729 N.W.2d 757 (Wis. App. 2007) (finding violation of open records law via disclosure of .pdf image files instead of provision of database access) <<http://www.wicourts.gov/ca/opinion/DisplayDocument.pdf?content=pdf&seqNo=27629>>.

²⁹⁶ For some federal agency retention requirements, see National Archives, *General Records Schedules* (July 24, 2007) <<http://www.archives.gov/records-mgmt/ardor/records-schedules.html>>. For issues impacting state governments generically, see this two-part series: NASCIO, *Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise* (July 2007) <<http://www.nascio.org/publications/pubsSubject2.cfm?category=30>>. Cf. NASCIO, *Seek and Ye Shall Find? State CIOs Must Prepare Now for E-Discovery!* (Sep. 5, 2007) <<http://www.nascio.org/publications/documents/NASCIO-EDiscovery.pdf>>. For an example of a set of retention requirements applicable to a state's agencies and local government entities, see California Secretary of State, *Local Government Records Management Guidelines* (Feb. 2006) <<http://www.sos.ca.gov/archives/locgov/localgovrm7.pdf>>.

²⁹⁷ *AMA 2006 Survey*, *supra* note 11.

²⁹⁸ See also Jacoby, Conrad, *Discovery of Employee-Owned Computer Equipment*, LLRX (Oct. 29, 2007) <<http://www.llrx.com/node/1934/print>>; cf. McCoy, Dan, *Out of Sight, Out of Mind, Into Court*, Nat'l L.J. (Jan. 17, 2007) <http://www.fenwick.com/docstore/Publications/Litigation/Out_of_Sight.pdf>.

litigation. Thus, legal issues regarding workplace electronic activity require careful, jurisdiction-specific analysis. There are two principles, however, that all employers should apply when considering acts which might arguably violate employee privacy: notice and reasonableness.

- **Notice**

Employers gain a valuable measure of protection by providing clear and specific notice to employees of their legitimate business interests and their resultant policies regarding screening, monitoring and investigating employees' conduct.

The benefits to be derived include:

1) Establishing the legitimacy and importance of their business interests and expectations by publicizing the same in employee handbooks and policy manuals

- *Example A:* If an employer believes that the company's "reputation" demands certain on-duty conduct (such as dress or behavior) and/or off-duty conduct (such as avoiding arrests, convictions or bad publicity), it can reduce risk.
- *Example B:* An employer may similarly enforce reasonable anti-nepotism and anti-conflict of interest policies.

2) Diminishing the privacy expectations of employees, perhaps enough to permit an employer to prevail in any subsequent dispute.

- *Example:* Company notice to employees that it will conduct certain kinds of inspections, like urinalysis, random car searches and locker searches.

3) Successful bargaining with labor unions to delineate privacy expectations and obtain consent to certain types of searches and seizures as a further way to reduce management risk.

- *Example:* Consent to urinalysis screening.

- **Reasonableness**

Employers should establish a reasonable and logical connection between the company's legitimate business interests and any employee conduct the company attempts to regulate. Intrusions into employee's electronic activity should be thoughtfully and reasonably administered.

Employers should establish a reasonable and logical connection between the company's legitimate business interests and any employee conduct the company attempts to regulate. Intrusions into employee privacy should be thoughtfully and reasonably administered. Thus, a drug store that might quite properly place a closed circuit monitor in

its pharmacy department would act unreasonably by placing a monitor in its locker or changing area. Employers may reasonably monitor the frequency of an employee's personal calls, but, in most cases, monitoring the contents will constitute an unreasonable invasion of privacy if the employee has a legitimate expectation of privacy in his or her phone calls.

Similarly, most jurisdictions deem pre-employment drug screening reasonable, but mandatory random screening of employees is often found reasonable only if the company can demonstrate other compelling factors such as safety or security concerns. Interrogation of employees should be handled in a deliberate, non-emotional fashion by giving employees notice of the employer's suspicions, an opportunity to respond and forewarning of the consequences attached to failure to respond rather than by confronting the employee in public and in an accusatory style.

If an employer wishes to use honesty or personality testing techniques, it should document its reasons for using the screening device and insure it is implemented in a reasonable and scientifically credible manner where permitted. In short, employers should act aggressively but not recklessly to protect their legitimate interests.

Finally, employers should avoid unnecessary and unwarranted intrusion into the off-duty activities of their employees. Employers should evaluate the reasonableness of their proposed intrusion into off-duty activities in light of the company's legitimate interests. When off duty intrusions are planned, such actions should also be carefully implemented in the least intrusive way possible.

- **Other Key Considerations**

In developing any written policy, some general themes and goals are:

- Develop fair, well-articulated, detailed policies;²⁹⁹
- Avoid the "Compliance Gap": Before drafting or revising, let alone rolling out, a policy or protocol . . . think through what realistically will happen "in the trenches."
- Search for "Gap Fillers" : synchronize the contents of pertinent respective provisions of related policies.
- Be open and honest with employees;
- Enforce policies as uniformly as possible;
- Respect individual privacy rights when the activity of the individual neither interferes with job performance nor entails any risk of corporate liability for employee conduct.

²⁹⁹ An employer's covert monitoring could potentially give rise to civil and even possibly criminal liability. For example, the Telephone Records and Privacy Protection Act of 2006 , criminalizes "pretexting" to obtain telephone records. 18 U.S.C. § 1039, Pub. L. No. 109-476 <<http://publaw109-476.notlong.com>>. The support for the legislation came in the aftermath of the spying scandal at Hewlett-Packard in which the company used private detectives to retrieve phone records of directors, managers and journalists in an effort to discover purported leaks to journalists from within its board. See Brad Stone and Matt Ritel, *Senate Passes Bill to Criminalize Pretexting*, N.Y. Times (Dec. 9, 2006) <<http://PretextingNYT120906.notlong.com>>.

- Determine what policies you want (e.g., Technology, E-mail & V-mail/Unified-Messaging; (Anti-)Blogging; Instant Messaging (IM) use or ban; Approval process for over-writing (re-imaging) departing employees' laptops and devices).³⁰⁰

B. Some Key Privacy-Related Policies

1. Policies Eliminating Employee Privacy Expectations

a. Computer Systems and Hardware Policies

An effective technology 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. In particular, the employer will want to delineate a broad scope, namely something to the effect that the Company owns "all information created, received or stored" on any "system, network, computer and mobile device provided or supported by the Company."³⁰¹

Generic log-on "banner" warnings as to "monitoring" may be insufficient, according to one 2006 decision in the government/military setting.³⁰² There, the context was a Fourth Amendment challenge to a search of a marine's e-mail contents in a criminal court-martial proceeding premised on drug charges. On appeal of a conviction, the Court of Appeals for the Armed Forces found these flaws in the Government's subjective *and* objective "expectation of privacy" arguments: (1) the banner's lack of establishment of the right "to engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system;" and (2) the user's password was

³⁰⁰ For some generic examples of policies, see Appendix D. See also the sample overview of an Acceptable Use Policy at Appendix C. Bearing in mind the time-honored caveat about over-reliance on generic "forms," see also Flynn, Nancy, *The ePolicy Institute™ ePolicy Forms Kit* (2d Ed. 2007), available for purchase at <http://www.epolicyinstitute.com/bin/loadpage.cgi?1234395343+forms/index.asp>. As to "social media" (a/k/a Web 2.0 and/or social-networking) policies in particular, see Jaffe, Jay M., *Setting a Social Media Policy*, eCommerce Law & Strategy (June 10, 2009) (linking to samples) <http://www.law.com/jsp/ca/PubArticleFriendlyCA.jsp?id=1202431342723>.

³⁰¹ See, e.g., SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 1, § I(B)-(D), at App. D-1; SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 2, § I; SAMPLE ELECTRONIC MAIL POLICY, § 1, at App. D-10. See generally Travis, *supra* note 7 ("Publish a Comprehensive Computer Use Policy" and "Integrate Computer Use Into Existing Policies"). 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.

³⁰² *U.S. v. Long*, 64 M.J. 57 (Sep 27, 2006) www.armfor.uscourts.gov/opinions/2006Term/05-5002.pdf, reconsideration denied by 64 M.J. 312 (U.S. Armed Forces Nov 7, 2006).

known only to her.³⁰³ Presumably it would have made a difference if the network administrators had had access to her password.

A vigorous dissent – citing, among other authorities, the *Garrity* decision discussed in Section II(B)(5) above – found the majority’s analysis severely flawed. Nonetheless, the *Long* decision underscores the importance not only of policies’ particular language but also of established custom in a given government workplace. As the *Long* majority emphasized in its required intensive analysis of the factual circumstances that the network administrator’s testimony had “repeatedly emphasized the agency practice of recognizing the privacy interests of users in their e-mail.”³⁰⁴

In *TBG Ins. Servs. v. Superior Court (Zieminski)*,³⁰⁵ 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.

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

³⁰³ *Id.* at 63, 64-65. In more typical factual contexts, at least several decisions have rejected employees’ privacy assertions:

[E]mployees do not have a reasonable expectation of privacy in the contents of their work computers when their employers communicate to them via a flash-screen warning a policy under which the employer may monitor or inspect the computers at any time. See [*U.S. v. Angevine*, 281 F.3d [1130,] 1132, 1135 [(10th Cir. 2002)]] (holding professor had no reasonable expectation of privacy in university computer where university computer policy, which was communicated in part via flash screen, “explains appropriate use, warns employees about the consequences of misuse, and describes how officials administer and monitor the University computer network”); *Haynes [v. A.G. of Kansas]*, 2005 WL 2704965, at *4 [(D. Kan. Aug. 26, 2005)] (finding plaintiff clearly “on notice that he did not have an expectation of privacy in [his work] computer and its contents” where warning to that effect was displayed every time plaintiff logged on to his computer); [*U.S. v. Bailey*, 272 F. Supp. 2d [822,] 831, 836 [(D. Neb. 2003)]] (holding plaintiff had no reasonable expectation of privacy in work computer where computer screen displayed a warning every time plaintiff logged onto his computer that his use of computer could be monitored).

U.S. v. Etkin, 2008 WL 482281, at *4 (S.D.N.Y. Feb. 20, 2008).

³⁰⁴ *Long*, 64 M.J. at 63, 64.

³⁰⁵ *TBG Ins. Servs. v. Superior Court (Zieminski)*, 96 Cal. App. 4th 443, 117 Cal. Rptr. 2d 155 (Cal. App. 2 Dist. 2002) <http://caselaw.lp.findlaw.com/data2/californiastatecases/b153400.pdf>.

drive even if the computer user does not actually visit any pornographic websites.³⁰⁶ However, if there is evidence – such as web search terms – of the suspect’s affirmative conduct, that is another story.³⁰⁷

In the context of 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, there is a growing body of decisional law addressing a former employee’s obligation to preserve the electronic-information status quo so that the

³⁰⁶ See, e.g., *Barton v. State*, 286 Ga. App. 49, 648 S.E. 2d 660, 663 (2007) (reversing conviction because presence of “pornographic images in . . . cache files . . . insufficient to constitute knowing possession . . . absent proof [of] . . . some affirmative action to save or download those images . . . or . . . knowledge that the computer automatically saved those files”), *cert. denied* (Sep. 10, 2007); Alyson M. Palmer, *Appeals Panel ‘Reluctantly’ Tosses Child Porn Case*, *Fulton Cty. Daily Rep.* (June 27, 2007) <<http://www.law.com/jsp/article.jsp?id=1182848790153>>. See also Imaeyen Ibang, *Teacher: Wrong Computer Click Ruined My Life*, *abc NEWS* (Jan. 27, 2009), <<http://abcnews.go.com/print?id=6739393>>; Rick Green, *Connecticut drops felony charges against Julie Amero, four years after her arrest*, *Hartford Courant* (Nov. 21, 2008) <http://blogs.courant.com/rick_green/2008/11/connecticut-drops-felony-charg.html>; Elinor Mills, *State worker cleared on child porn charges that were due to malware*, *c/net* (June 17, 2008) <http://news.cnet.com/8301-10784_3-9970660-7.html>; Lindsay Beyerstein, *Questionable Conviction of Connecticut Teacher in Pop-up Porn Case* (*AlterNet* Jan. 19, 2007) <<http://www.alternet.org/module/printversion/46925>>. Cf. *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006) (sentence reduced because vast majority of child-pornography images ended up in cache without action or knowledge of Defendant-user) <[http://www.ca9.uscourts.gov/ca9/newopinions.nsf/854C325F83310DBF88257233005978B3/\\$file/0530607.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/854C325F83310DBF88257233005978B3/$file/0530607.pdf?openelement)>.

³⁰⁷ *State v. Hurst*, 2009 WL 580453, *10-*11 (Ohio App. 5 Dist. Mar. 6, 2009) (affirming conviction because “state presented sufficient evidence to establish that appellant sought out the images and exercised dominion and control over them” and “[a]ppellant’s use of search terms to certain types of websites demonstrate[d] his affirmative actions to obtain certain images and place them on his computer screen”) <<http://www.sconet.state.oh.us/rod/docs/pdf/5/2009/2009-ohio-983.pdf>>; *Tecklenburg v. App. Div.*, 169 Cal. App. 4th 1402, 87 Cal. Rptr. 3d 460, 473 (Cal. App. 3 Dist. Jan. 8, 2009) (upholding conviction; “defendant . . . actively searched for child pornography Web sites, . . . went past the home pages, clicked through images on at least one site tour, display[ing] multiple images . . . in some cases multiple times, and enlarg[ing] some of the images from thumbnail views”) <www.courtinfo.ca.gov/opinions/documents/C055368.PDF>, *review denied* (Apr. 1, 2009); *State v. Jensen*, 173 P.3d 1046, 1052 (Ariz. App. Div. Jan. 15, 2008) (“the presence of two images in the temporary internet folder and the image in the unallocated cluster, coupled with the numerous syntax searches for words and phrases associated with child pornography, is evidence of voluntary action undertaken by the computer operator in an effort to receive child pornographic images. . . .”) <<http://www.cofad1.state.az.us/opinionfiles/cr/cr06%2D0376.pdf>>. See generally David Frey, *Computer Crime: Prosecuting Child Pornography*, *N.Y.L.J.* (Apr. 17, 2009) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202429968700>>.

court and the former employer can follow the digital trail.³⁰⁸ 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.³⁰⁹

The employers' overall right to inspect work-provided computers that are physically in the office is typically much more straightforward. Usually, a physical lock on an employee's office door is of no consequence. Yet one anomalous circuit court merits some discussion. In *U.S. v. Ziegler* ("*Ziegler I*"),³¹⁰ the Ninth Circuit initially concluded that an employer's widely-known policy/practice of monitoring employee computer and internet activity defeated the employee's claim that he had a reasonable expectation of privacy in his computer use.³¹¹

³⁰⁸ In addition to the *Krumwiede* and *Kucala* decisions cited in footnote 58 above, see *Anadarko Petroleum Corp. v. Davis*, 2006 U.S. Dist. LEXIS 93594 (S.D. Tex. Dec. 28, 2006) <https://ecf.txsd.uscourts.gov/cgi-bin/show_case_doc?case_id=470305&doc_num=46&de_seq_num=132&pdf_header=0> (denying sanctions against ex-employee); *Plasse v. Tyco Electronics Corp.*, 448 F. Supp. 2d 302 (D. Mass. Sep. 7, 2006) ("*Plasse I*") <https://ecf.mad.uscourts.gov/cgi-bin/show_case_doc?51.91257,,,,,176.1>, as supplemented by, *Plasse v. Tyco Electronics*, 2006 U.S. Dist. LEXIS 89829 (D. Mass. Nov. 8, 2006) ("*Plasse II*") (sanctions included dismissal of all claims brought by former employee) <https://ecf.mad.uscourts.gov/cgi-bin/show_case_doc?58.91257,,,,,200.1>; *Dodge, Warren & Peters Ins. v. Riley Serv, Inc.*, 130 Cal. Rptr. 2d 385 (Cal. App. 4 Dist. 2003) (issuing a "freeze" order to "preclude the innocent or intentional alteration or destruction of evidence" as to electronic files taken from former employer when the defendants had left to open their own company) <<http://caselaw.lp.findlaw.com/data2/californiastatecases/e031719.pdf>>. Cf. *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) <<http://www.ca6.uscourts.gov/opinions.pdf/08a0226p-06.pdf>>; *Regan-Touhy v. Walgreen Co.*, 526 F.3d 641 (10th Cir. 5/20/08) (affirming district court's denial of "kitchen sink" motion to compel production of access log files and of all operating manuals for all potentially pertinent systems and programs) <<http://www.ca10.uscourts.gov/opinions/06/06-6242.pdf>>.

³⁰⁹ *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>>.

³¹⁰ *U.S. v. Ziegler*, 474 F.3d 1184 (9th Cir. Jan. 30, 2007) ("*Ziegler I*") <<http://www.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 lengthy set of opinions, one concurring and two dissenting) <<http://www.ca9.uscourts.gov/datastore/opinions/2007/06/20/0530177o.pdf>> ("*Ziegler III*"), *cert. denied*, 128 S. Ct. 879 (2008). Cf. *U.S. v. Barrows*, 481 F.3d 1246 (10th Cir. 2007) (city employee, convicted of child pornography possession, had no reasonable expectation of privacy for Fourth Amendment purposes in personal computer he had brought to city office, networked to a work computer, kept running all the time and on which he did all his work) <<http://www.ca10.uscourts.gov/opinions/06/06-6274.pdf>>; *Wilson v. Moreau*, 440 F. Supp. 2d 81 (D.R.I. 2006) (in public employee context, distinguishing workplace computer from password-protected personal e-mail account) <https://ecf.rld.uscourts.gov/cgi-bin/show_case_doc?131,4905,,,,,696145,1>.

³¹¹ *U.S. v. Ziegler*, 456 F.3d 1138 (9th Cir. 2006) ("*Ziegler I*") , *superseded by Ziegler II*.

The employee, Ziegler, worked as the director of operations for Frontline, an online payment processing company. Frontline's internet service provider alerted the FBI of child porn-related internet searches on the company's account. After the employer helped the FBI trace the activity to Ziegler's computer, the FBI arrested him. At his criminal trial, Ziegler moved to suppress the electronic evidence, arguing that he had a reasonable expectation of privacy on his work computer.

At the appellate stage, upon rehearing, the Ninth Circuit broke with the majority view on this issue³¹² by holding that Ziegler *did* retain a legitimate expectation of privacy in his "private" workplace office because he did not share his office with any co-workers and kept the door locked.³¹³

However, the *Ziegler II* court then found that the employer retained the ability to consent to a search of the contents of the hard drive of Ziegler's workplace computer. Why? "[T]he computer is the type of workplace property that remains within the control of the employer 'even if the employee has placed personal items in [it].'"³¹⁴

Although use of company computers was subject to an individual log-in, the company's IT department had complete administrative access to anybody's machine.³¹⁵ The

³¹² For example, in *Biby v. Board of Regents of Univ. of Nebraska at Lincoln*, 419 F.3d 845 (8th Cir. 2005) <<http://caselaw.lp.findlaw.com/data2/circs/8th/043878p.pdf>>, the employee helped to develop a credit card technology that the University of Nebraska later licensed to a third party manufacturer. Later, the University and the third party manufacturer were arbitrating a dispute over the license. As a result of the arbitration, the University notified Biby that it would have to access his email files. After the arbitration, the University terminated Biby, who then sued for invasion of privacy. The court held that Biby did not have a reasonable expectation of privacy in his computer files, primarily because the university computer policy had put him on notice that he should have had no such expectation if the university had a legitimate reason to search his files. For a more recent similar decision in a different context, see *Cowles Pub. Co. v. Kootenai County Bd. of County Com'rs*, 144 Idaho 259, 159 P.3d 896 (2007) (e-mails between public employees were public records and, due to signed County e-mail policy, were not protected by legitimate privacy expectation) <<http://www.isc.idaho.gov/opinions/cowles14.pdf>>.

Compare *Bourke v. Nissan Motor*, No. B068705 (Cal. App. 2 Dist. July 26, 1993) (unpublished) <http://www.loundy.com/CASES/Bourke_v_Nissan.html>. There, the employer randomly selected a message from its e-mail system as part of an employee training exercise. The message, sent by employee Bourke, included personal and sexual content. Based on this discovery, Nissan reviewed all of the messages sent by employees in Bourke's group. Nissan found substantial numbers of personal, including sexual, messages from Bourke. It then issued written warnings to the employee for violating the company policy prohibiting the use of the company computer system for personal purposes. Bourke sued Nissan for invasion of privacy, claiming that because the system allowed employees to password-protect their e-mail access, they had a legitimate expectation that their e-mail would be private. The court rejected Bourke's claim, finding that any expectation of privacy was not reasonable because the employees knew the messages could be read by people other than the intended recipients.

³¹³ 474 F.3d at 1190.

³¹⁴ *Id.* at 1191.

³¹⁵ *Id.*

company had also installed a firewall allowing it to monitor Internet traffic.³¹⁶ Monitoring was routine, and the IT department reviewed the log created by the firewall regularly, sometimes daily.³¹⁷ In addition, upon hiring, employees were notified of the company's monitoring efforts through training and an employment manual, and were told that the computers were company-owned and not for activities of a personal nature.³¹⁸

In that context, the court found Ziegler "could not reasonably have expected that the computer was his personal property, free from any type of control by his employer."³¹⁹ Thus, the employer could consent to a search of the office and the computer that it had provided to Ziegler.³²⁰ Because evidence was seized pursuant to a valid consent to search given by the employer, the court denied suppression of the pornographic evidence.³²¹

Yet another decision in this context arose in response to a motion to suppress evidence in a criminal case. In *U.S. v. Hassoun*,³²² a Florida federal district court synthesized *Long* and *Ziegler I* by holding that a policy's lack of a prohibition on all personal use does not undo a clear policy provision regarding monitoring. Consequently, in affirming a magistrate judge's denial of the motion to suppress, the *Hassoun* court distinguished *Long* on its "unique" facts and quoted *Ziegler I* to the effect that: "Employer monitoring is largely an assumed practice, and thus . . . a disseminated computer-use policy is entirely sufficient to defeat any expectation that an employee might nonetheless harbor."³²³

b. Inspection/Litigation Provisions

Contracts 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.³²⁴ Moreover, as soon as there is concern that a particular employee may bring a claim, an employer should consider obtaining a forensically sound image of each computer and laptop provided to that employee.³²⁵ Similarly, where misappropriation

³¹⁶ *Id.*

³¹⁷ *Id.* at 1192.

³¹⁸ *Id.*

³¹⁹ *Id.*

³²⁰ *Id.*

³²¹ *Id.* at 1193.

³²² *U.S. v. Hassoun*, 2007 WL 141151, *2 (S.D. Fla. Jan. 17, 2007).

³²³ *Id.*

³²⁴ See the *TBG*, *Biby* and *Bourke* decisions discussed in the preceding sub-section.

³²⁵ *Henry v. IAC/Interactive Group*, 2006 U.S. Dist. Lexis 80307 (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 forensics decisions cited and linked in footnotes 58 and 308-309 above.

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,³²⁶ 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. 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.³²⁷

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.³²⁸ Their coverage should include voicemail, IM, PDA's, and other company-issued mobile devices. This issue recently came to the fore when incoming President Barack Obama ostensibly had to negotiate with his own staffers as

³²⁶ See, e.g., *Copland v. United Kingdom*, (European Court of Human Rights 7/3/07) (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://cmiskp.echr.coe.int/tkp197/viewhbk.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=61533&sessionId=1825040&skin=hudoc-en&attachment=true>>.

³²⁷ 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") <www.export.gov/safeharbor/SafeHarborInfo.htm>.

³²⁸ Citizens for Responsibility and Ethics in Washington (CREW), Press Release (linking to Letter to U.S.A.G.) (Feb. 4, 2008); see also Williamson, Elizabeth and Eggen, Dan, *White House Has No Comprehensive E-Mail Archive*, Wash. Post (1/22/08).

to the conditions under which he ultimately got to keep his beloved Blackberry.³²⁹ 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.³³⁰

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

a. What Position Should My Organization Take With Respect To Blogs, Social-Networking Sites and the Like?

Determining an organization's official position on employee web postings is a much harder task than it appears at first glance. The spectrum of positions ranges from (1) actively encouraging employees to create and maintain content by providing them with the tools necessary to do so to (2) providing guidance about proper posting of content to (3) flat out prohibiting such postings (that approach could be illegal in certain circumstances).

To determine where your 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

³²⁹ See, e.g., Scheer, Peter, *The View – Will Obama's Handlers Force Him to Hold the Phone*, L.A./S.F. Daily Journal (Jan. 26, 2009), available at <<http://www.carealestatejournal.com/newswire/components/printArticle.cfm?sid=&tkn=&eid=899298&evid=1&scid=>>>; Zeleny, Jeff, *For a High-Tech President, a Hard-Fought E-Victory*, N.Y. Times (Jan. 23, 2009) <www.nytimes.com/2009/01/23/us/politics/23berry.html?pagewanted=print>; Declan McCullagh, *First e-mailing prez: Obama keeps his BlackBerry*, c.net (Jan. 22, 2009) <http://news.cnet.com/8301-13578_3-10148329-38.html>; Ambinder, Mark, *Obama Will Get His BlackBerry*, Atlantic (Jan. 21, 2009) <http://marcambinder.theatlantic.com/archives/2009/01/obama_will_get_his_blackberry.php>; Stone, Brad, *The High Security Risk Attached to Obama's Belt*, N.Y. Times (Jan. 12, 2009) <<http://www.nytimes.com/2009/01/12/technology/internet/12blackberry.html?pagewanted=print>>; McComas, William A., *Risky for all executives*, Nat'l L.J. (Jan. 5, 2009) <<http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202427103848>>; Zeleny, Jeff, *Lose the BlackBerry? Yes He Can, Maybe*, N.Y. Times (Nov. 16, 2008) <http://www.nytimes.com/2008/11/16/us/politics/16blackberry.html?_r=1&sq=Obama%20may%20have%20to%20give%20up%20BlackBerry&st=cse&scp=1&pagewanted=print>.

³³⁰ See, e.g., Ted Bridis, *Phones Spill Secrets of Previous Users*, AP (Aug. 30, 2006) <<http://www.msnbc.msn.com/id/14588433>>; *Used Smartphones and PDA's for Sale on eBay Reveal Massive Volume of Sensitive Data*, Trust Digital (Aug. 30, 2006) ("loaded with sensitive personal and corporate information") <http://www.trustedigital.com/news/press/2006_0830.asp>.

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 recent 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 is appropriate for elected legislators to be interacting with constituents via social-networking sites.³³¹ When the public employees in question are not legislators, though, what do you think your agencies and/or clients should do in this regard?

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.

b. What Options Does My Company Have For Telling Employees Its Position On Web Postings?

Whether a company need a “blog (and social-networking/Twittering) policy depends. Not every company needs an independent policy on employee blogs, although updating of the company’s current policies might be in order.

(i) Rely on Existing Policies

The following policies, which a company is likely to already have, provide guidance to employees about some of the legal issues raised above:

- (a) *Code of Conduct and/or Ethics:* as to proper communications and not revealing sensitive financial information;

³³¹ Helderman, Rosalind S., *Legislators Log Back On To Facebook*, Wash. Post (Feb. 11, 2009) <www.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) <<http://www.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) <www.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) <http://news.cnet.com/8301-1009_3-10078353-83.html>.

(b) *Internet and Computer Use Policy*: as to electronic communications, use of company equipment, personal use during business hours, and notification of monitoring computer and Internet usage;

(c) *Anti-Harassment and Equal Employment Opportunity Policies*: as to appropriate (and inappropriate) content;³³² and

(d) *Confidential and Trade Secret Information Policy*: as to appropriate (and inappropriate) content.

There is risk, however, in relying on existing policies: while such policies generally address appropriate (and inappropriate) conduct, bloggers may not realize that their personal blogs can affect *their employer and their work environment*. One of the major protests of employees terminated based on the content of their blogs tends to be an alleged lack of notice that their conduct was inappropriate.

(ii) **Revise Existing Policies to Reference Blogs**

While an employer's existing policies likely already address some issues implicated by personal blogs, revisions to those existing policies may be necessary to drive home the relevance of those policies to an employee's off-duty conduct. Such revisions can be as simple as including a reference to "an employee's personal web log or blog" in the Internet and Computer Use Policy and an example of a harassing blog in the Anti-Harassment Policy. Or, a company may decide to add a short "Blog" component to its Internet and Computer Use Policy. Such a component should emphasize the following:

- Blogs have more permanence than they appear. Technology, as evidenced by the WayBack Machine and Google's cached archive, permits retention of blog content even after the author deletes such information. So, employees should be careful what they commit to a blog.
- Exercise common sense and respect others. Blogs, unless restricted, are available for anyone to read. Employees should assume that people will read their blogs. One test suggested for evaluating the appropriateness of the content is whether the blogger would be embarrassed if his or her parent or young child read the blog.

Speak for yourself. Employees do not represent the company and should refrain from attempting to speak on its behalf. In addition, employees should be very cautious about references to the employer since the content of the blog and the context of the employer-related references could impact the company and its business.

³³² Cf. Michelle Yoffee-Beard, *Oviedo officer resigns after online sex ads, photos uncovered*, Seminole Chronicle (Aug. 6, 2008) <<http://www.seminolechronicle.com/vnews/display.v/ART/2008/08/06/489a38bf11c0e>>; Ian Shapira, *When Young Teachers Go Wild on the Web; Public Profiles Raise Questions of Propriety and Privacy*, Wash. Post (Apr. 28, 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/27/AR2008042702213_pf.html>.

(iii) Supplement Existing Policies with a Blog Policy

Some companies may decide to supplement their current policies with a full-fledged, independent policy on blogs. This approach would be highly recommended for a company that decides to encourage employees to blog – either for personal or corporate reasons. An independent policy would typically also be a necessity for an employer that decides to provide the tools and resources to assist employees in their creation of personal or corporate blogs.

For a company that wishes to provide guidance to employees about the appropriate content for their blogs,³³³ the Weblog Policy should contain the following components:

- *Employee's Identification of Personal Views:* An employee should clearly identify to readers, through a disclaimer or otherwise, that the views expressed are those of the employee and not necessarily of the company. Even though the company views the blog as the employee's personal project and expression, the content and context of references to the company may create a different impression for some readers. Using reasonable efforts to draw a reader's attention to the disclaimer should help clear up any confusion.
- *Protection the Company's Confidential Information:* An employee must refrain from disclosing the confidential or proprietary information of the company and of any third party that has disclosed information to the company. Presumably, the company maintains a policy about confidential information and requires all employees to sign Employee Confidential Information and Invention Assignment Agreements; if so, the policy can repeat the definition of confidential information to remind employees of the scope of information that should not be disclosed, referencing the policy and the agreement. Further, the agreement provides the employer certain rights regarding concepts and inventions employees create that are related to the company's business. Employees should be admonished to consult their managers before disclosing any such concepts or invention. Finally, the policy should highlight that revelation of certain sensitive information can result in violation of securities laws.
- *Exercise of Common Sense and Respect for Others.* Blogs, unless restricted, are available for anyone to read. Employees should assume that people will read their blogs. Employees should abide by the employer's Code of Conduct and other conduct-related workplace policies (such as the Anti-Harassment and Equal Employment Opportunity Policies) when blogging, especially if such blogs are associated, in any way, with the company. Employees should respect others' privacy.
- *Employer Reservation of Rights:* The Company should retain discretion to determine if a particular website or blog violates this policy and reserve the right to request an employee temporarily refrain from commenting on topics related to the company (or, in rare instances, suspend the website or blog altogether) if advisable to comply with securities or other laws.

³³³ See generally Alan Cohen, *Keeping Secrets; Strong Internal Policies Can Allow Firms to Reap the Benefits of Blogs – And Avoid Getting Burned*, 6/2007 Am. Law. 71.

- *Contact for Follow Up Questions:* The Company should designate a contact person for questions related to this policy. Frequently, companies rely on the Human Resource Manager as the contact for any policy-related questions.

Companies may also wish to address (1) use of company equipment in accessing, updating, and storing personal blogs; (2) limits on personal blogging on company time and company-related blogging for non-exempt employees to company time; (3) linking to the company website; (4) an admonishment not to reference customers or partners without their prior approval; and (5) an admonishment not to use others' copyrighted materials.

Enclosed as part of the attached Appendix D, at D-15 to D-16, is a sample geared to the company that recognizes employees will likely blog (with or without company blessing) and wishes to provide guidance as to appropriate conduct.

Companies that – in addition to encouraging blogging – provide the tools and resources for employees to create blogs on company servers, should consider a more fulsome policy. Such a policy would also explain the company's purpose in encouraging employees to create blogs and identify the employer expectations regarding use of the blogs. For example, one employer may wish to use blogs to facilitate open communication between customers and the company, while another may encourage employees to blog so that they become familiar with the technology and stay on the forefront of technological advances. Either way, the purpose for encouraging employees to blog will likely inform how the company and its legal counsel draft various of the above-listed components of the policy.

(a) Additional Documentation

Companies may also wish to consider obtaining an acknowledgment that the employee received and read the new policy and/or requiring a usage agreement (in connection with employer-provided tools and resources to create blogs).

(b) Supplement Training Materials

A company may also communicate its position about blogging by modifying training it already provides to employees. For instance, California law requires most employers to conduct interactive sexual harassment training sessions.³³⁴ One way to alert employees about potential liability arising from a blog is to include examples of harassing content in the sexual harassment training session. Further, some companies provide training about appropriate use of company equipment and/or electronic communications. If so, the company should include blogs as an example of an electronic communication and should emphasize that the same policies governing computer usage and appropriate email conduct apply with equal force to blogs.

³³⁴ See Cal. A.B. 1825, Cal. Gov't Code § 12950.1, requiring employers to provide two hours of sexual harassment training to all supervisory employees by January 1, 2006 and thereafter every two years. The law applies to employers who have 50 or more employees or who receive services from 50 or more contractors.

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. At least in the harassment context, failure to do so may result in potential vicarious liability to third parties – based on actual or constructive knowledge of an employee's harmful activities plus the employer's failure to remedy the behavior.

Harassment is not the only arena for concern. For example, in *Doe v. XYZ Corp.*,³³⁵ the court found that an employer on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has heightened duties. It must investigate and take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. "No privacy interest of the employee stands in the way of this duty."³³⁶

In *Doe*, an employee's wife brought a negligence action against her husband's former employer to recover damages allegedly suffered by her and her 10-year old daughter. The mother sought to hold the employer liable for damages caused by her husband's use of his workplace computer to send nude photographs of the girl (his stepdaughter) to pornographic websites. The employer was aware that the employee had a minor stepchild, although it did not know that he was uploading and transmitting inappropriate pictures of that child.

The court found that the company's policy permitted it to monitor its employees' use of work computers and discipline employees for use of work computers for non-business activities. The employer also owned software that permitted it to determine which websites employees were visiting. Furthermore, the court noted that the employee's supervisors had actual knowledge that the employee improperly used his company computer to view pornographic websites. In response, the employer asked the employee to stop visiting inappropriate websites. Yet, the employee continued to do so; and, despite additional complaints by other workers, no further action was taken.

Eventually, the employee was arrested for possession of child pornography, based in part on photographs of the child found in the employer's dumpster. The child's mother sued the employer, claiming that the company was responsible for the harm suffered by her child because it knew or should have known that the employee used his company computer to transmit child pornography, but it failed to report such crimes. The mother alleged that the employer had a duty to report the employee to the proper authorities upon discovering the crimes he committed on company property.

The New Jersey appellate court held that the mother's claim was valid. The court reasoned that the employer's knowledge warranted investigation of the employee's activities

³³⁵ *Doe v. XYZ Corp.*, 887 A.2d 1156 (N.J. Super. A.D. 2005)
<<http://lawlibrary.rutgers.edu/decisions/appellate/a2909-04.opn.html>>.

³³⁶ 887 A.2d at 1158.

to determine if they constituted illegal acts, such as viewing child pornography. In so deciding, the court made the following conclusions:

- Upon being put on notice of the employee's improper behavior, the employer had a duty to: (1) investigate his activities; (2) take prompt action to stop any unauthorized acts; and (3) report it to the proper authorities;³³⁷
- No privacy interest of the employee stood in the way of the employer's duty to investigate and take action.³³⁸

The court fell short of imposing liability on the employer, and instead remanded the case to the trial court to determine whether the employer's breach of duty was the proximate cause of the harm to the child.

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.³³⁹ In *Dep't Of Education v. Choudhri*,³⁴⁰ the employer claimed that its employee was insubordinate because of the employee's non non-business Internet use. The employee argued that he: only Web-surfed after completing all of his work and while waiting for more work; and never neglected work assignment.³⁴¹ *Choudhri* found that selective enforcement of the prohibition on using the internet for any personal reasons was "unusually harsh and arbitrary, motivated by anger rather than a concern for office productivity." Incidental use of the Web for a "non-work-related matter" – such as "to check the weather or find the location of a store" was "a minor transgression."³⁴²

³³⁷ *Id.* at 1166-69.

³³⁸ *Id.* at 1166.

³³⁹ Compare the NLRA issue discussed in Section II(B)(4) above.

³⁴⁰ OATH Index No. 722/06 (N.Y.C. Office Of Admin. Trials & Hearings Mar. 9, 2006) <<http://files.findlaw.com/news.findlaw.com/hdocs/docs/nyc/doechoudri30906opn.pdf>>.

³⁴¹ *Id.* at 13.

³⁴² *Id.* (emphasis added) (finding selective "prohibit[ion on one employee's] using the internet for any personal reasons was . . . motivated by anger rather than a concern for office productivity").

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.³⁴³

The law in this area is still in its nascent stage. Thus, in general, one option is to craft policies so that they lay the groundwork for 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.³⁴⁴

D. Periodic Training

Some identify the fundamental principles of policy implementation as “The Three E’s,” namely Establish, Educate and Enforce.³⁴⁵ Thus, once having developed written policies, employers should provide periodic training on the contents of such policies and of related protocols. The training should have a rules-of-law underpinning as well as an Information Technology (IT) component. It should 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 of the key subject areas should include e-mail “netiquette” as well as privilege/confidentiality.

1. E-mail “Netiquette” (Writing For Multiple Audiences)

Workers should be taught to be circumspect about what they put in writing, especially in e-mail. The “writing for multiple audiences” concept takes on added meaning in the e-mail setting. The capacity for e-mail to proliferate and end up all over the world raises the stakes greatly. In this regard, the author's firm cautions clients' employees via a proprietary “Green

³⁴³ *Nickolas v. Fletcher*, 2007 U.S. Dist. LEXIS 23843 (E.D. Ky. Apr. 12, 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). 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.

³⁴⁴ See, e.g., 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.

³⁴⁵ 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>>.

Eggs and Ham” mantra.³⁴⁶ Examples of inappropriate e-mail content include sexual imagery; defamatory language, “name-calling;” and discussion of predatory acts.³⁴⁷

2. Attorney-Client Privilege

A lawyer should train employees as to 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); avoiding excessive forwardings, re-distributions and “replies to all;” and refraining from re-stating counsel’s legal advice.

E. INFORMATION-SECURITY COMPLIANCE CONSIDERATIONS

Though a full-fledged discussion of information-security best practices is well beyond the scope of this paper, some mention is warranted of IT compliance frameworks and of metadata-handling protocols.

1. IT Compliance Frameworks

Data leakages can occur in many different ways, including hacking of networks,³⁴⁸ loss or theft of mobile devices such as laptops and iPods,³⁴⁹ improper disposal³⁵⁰ enabling

³⁴⁶ Available on request from the author. See generally Helen Leah Conroy’s *Resources* (e.g., “Ten Ways E-Mail Can Sabotage Your Business Negotiations”) <http://www.helenconroylaw.com/law_resources/resources.htm>; Nancy Flynn, *ePolicy Institute’s materials* (e.g., “Managing E-Risks to Keep Your Employees In-Line and Your Organization Out of Court”) <<http://web.archive.org/web/20071020225302/http://www.epolicyinstitute.com/speakers/topics.html>>.

³⁴⁷ Violent or war imagery can be particularly problematic. Sports language could be as well.

³⁴⁸ See, e.g., Jordan Robinson, Google halts ‘hijacked’ ads used to steal personal data, AP (Apr. 27, 2007) <http://www.siliconvalley.com/news/ci_5762859>.

³⁴⁹ Chris Jenkins, *Laptop lock down*, Australian IT (May 8, 2007) <<http://australianit.news.com.au/common/print/0,7208,21675095%5E15385%5E%5E%5Enbv%5E,00.html>>; Cara Garretson, *Five ways to prevent data theft by iPod; Options include endpoint security and plain old education*, NWW (Apr. 9, 2007) <<http://www.networkworld.com/news/2007/040907-prevent-ipod-data-theft.html>>; Cara Garretson, *Security fears grow as iPods proliferate; Apple’s storage-heavy iPods are security threat, but safeguards exist*, NWW (Apr. 9, 2007) <<http://www.networkworld.com/news/2007/040907-ipod-company-security.html?nwwpkg=ipod>> Ryan Sulkin, *First Line of Defense Against Data Security Breaches: Employees*, Employment Law Strategist (Dec. 29, 2006) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1167300412497>>.

³⁵⁰ Fair/Accurate Credit Transactions Act (FACTA) § 216, 15 U.S.C. 1681w(a)(1) <<http://15USC1681w.notlong.com>>; FTC’s Disposal Rule (June 1, 2005) <<http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf#page=32>>.

dumpster-diving,³⁵¹ human error,³⁵² employees' internet activity³⁵³ and phishing schemes.³⁵⁴ Yet, IT processes tend to be insufficiently controlled.³⁵⁵

Employers of all sorts can improve their information-security practices by focusing on the "CIA" (Confidentiality, Integrity and Availability) of electronic data.³⁵⁶ There are three major frameworks providing guidance for electronic information management.³⁵⁷ As to security breaches – and avoiding the painful and costly notifications to those impacted –

³⁵¹ Tim Gray, *Radio Shack Sued for Exposing Customer Info*, eCommerce Times (Apr. 3, 2007) <<http://www.ecommercetimes.com/story/56685.html>>.

³⁵² See, e.g. Bob Lewis, *Computer security when travelling by train – an expert's observation*, Computer Weekly (Oct. 21, 2008) <www.computerweekly.com/Articles/ArticlePage.aspx?ArticleID=232765&PrinterFriendly=true>

³⁵³ See Section I(B)(2)(a)-(b) above.

³⁵⁴ Brian Krebs, *Data Breach Aided University Phishing Scam*, Wash. Post (Apr. 16, 2007) <http://blog.washingtonpost.com/securityfix/2007/04/data_breach_may_have_aided_uni_1.html>.

³⁵⁵ Robertson, Jordan, *Your next high-tech gadget may come bundled with an extra – a virus*, AP (3/13/08) <<http://abcnews.go.com/print?id=4446944>>; Gage, Deborah, *Virus from China the gift that keeps on giving*, S.F. Chronicle (2/15/08) <<http://Digital-Frames-SFChron-2-15-08.notlong.com/>>.

³⁵⁶ See generally Jim Rapoza, *12 Ways to Be A Security Idiot*, eWeek (2003) <www.eweek.com/slideshow/0,1206,a=205467,00.asp?kc=EWPRDEMNL041807EOAD>. See also Lynn Tan, *Four deadly security sins*, ZDNet Asia (Nov. 6, 2007); <www.zdnetasia.com/news/security/printfriendly.htm?AT=62020417-39000005c>; Jaikumar Vijayan, *Six Ways to Stop Data Leaks*, Computerworld (Mar. 19, 2007) <<http://computerworld.com/action/article.do?command=printArticleBasic&articleId=285138>>; Ericka Chickowski, *Organizations turn to new techniques to fight financially motivated attacks*, SC Magazine (Feb. 15, 2007) <<http://Chickowski-2-15-07.notlong.com>> (citing M. Palmer, *STAYING PROACTIVE: Keeping tabs on data*, Cybertrust (2007) <http://www.itpolicycompliance.com/research_reports/data_protection/read.asp?ID=9>. For an example of an extremely deficient approach to information-security, see Andrew Clevenger, *Lawyer admits computer breach; [s]pying on firm may cost license*, Charleston Gazette (Mar. 2, 2008).

³⁵⁷ IT Infrastructure Library (ITIL) (best practices for it service management and delivery) <<http://www.itil.co.uk/http://www.itil.co.uk/>>; ISO 27002 (formerly ISO 17799); (security requirements) <<http://www.standardsdirect.org/iso17799.htm>>; Control Objectives for Information and Related Technology (COBIT) <<http://COBIT.notlong.com>>. See also ITGI & OGC, *Aligning COBIT®, ITIL® & ISO 17799 for Business Benefit* (2005) <<http://Aligning.notlong.com>>.

there are particular best practices required for federal agencies³⁵⁸ and additional ones that can help public universities.³⁵⁹

To be successful, 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).

2. Metadata-Handling and Redaction Protocols

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.³⁶⁰ Microsoft’s Word, Excel and PowerPoint menu options and its free batch removal tool entail many steps and are not sufficiently thorough.³⁶¹ Two affordable, user-friendly tools are Payne Consulting Group’s Metadata Assistant and Workshare’s Protect.³⁶²

³⁵⁸ OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007) <www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>; OMB, *Recommendations for Identity Theft Related Data Breach Notification* (Sep. 20, 2006) <www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf>; OMB, *Protection of Sensitive Agency Information*, M-06-16 (June 23, 2006) <www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>.

³⁵⁹ Privacy Rights Clearing House, *My Social Security Number: How Secure Is It?* <www.privacyrights.org/fs/fs10-ssn.htm> (“How can a school use my Social Security number?”); Mike Charbonneau, *ECU Mistakenly Posts Personal Info Online*, WRAL.com (Feb. 9, 2007) <www.wral.com/news/local/story/1198897/>.

³⁶⁰ See Section I(B)(2)(c) above. See generally Brownstone, Richmond JOLT, *supra* note 3, at 9-11, 41. Related concerns include: protecting confidential parts of documents via effective redaction methods, Robert D. Brownstone, Todd R. Gregorian and Michael A. Sands, *Secrets Easily Leaked by Friend or Foe In Publicly Filed .PDF Documents*, 13 No. 1 Cyberspace Lawyer 1 (West Jan./Feb. 2008), available on request from Robert D. Brownstone (citing Declan McCullagh, *AT&T leaks sensitive info in NSA suit*, c/net (May 30, 2006) <http://news.com.com/2102-1028_3-6077353.html?tag=st.util.print> (linking to improperly redacted brief, <www.politechbot.com/docs/att.not.redacted.brief.052606.pdf>)); Christopher S. Rugaber, *Error by FTC Reveals Whole Foods’ Trade Secrets*, AP (Aug. 15, 2007) <<http://Redact-FTC-WPost-8-15-07.notlong.com>>; and .pdf security, <<http://pdf-security-adobe.notlong.com>>. Cf. Opinion 701, N.J. Adv. Comm. on Prof’l Ethics (Apr. 24, 2006) (*dicta* that, because it is “not possible to secure the Internet itself against third party access,” lawyers should secure .pdf files via passwords) <http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html>.

³⁶¹ NSA, *Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF* (Feb. 2, 2006) <www.nsa.gov/snac/vtechrep/I333-TR-015R-2005.PDF>.

³⁶² <www.payneconsulting.com/products/>; <www.workshare.com/solutions/risk/metadata-hidden-data.aspx>.

Workplace Privacy Policies



NELI

Public Sector & EEO

August 28, 2009

San Francisco



© FENWICK & WEST LLP



Robert D. Brownstone, Esq.

Agenda; Sub-Topics Highlighted in Slides



- **I. INTRO – THE MODERN LANDSCAPE**
 - *Strange Things (Prospective) Employees Memorialize*
- **II. MONITORING OF EMPLOYEES’ ELECTRONIC ACTIVITIES**
 - *Some Justifications and Some Countervailing Concerns*
- **III. INVESTIGATIONS AND BACKGROUND CHECKS**
 - *Legality and Advisability of Following the Internet Trail*
- **IV. SEARCHING, SURVEILLING AND TRACKING PHYSICAL CONDUCT AND LOCATIONS**
 - *Workplace & Personal Searches*
 - *“Off-Duty” (Web) Activities*
- **V. IMPLEMENTING LEGALLY-COMPLIANT AND DEFENSIBLE POLICIES *(time permitting)***
 - *Three E’s; Risks/Benefits; Web-2.0/UGC*

I. Intro – The Modern Landscape

A. Our Digital World



- **TWO KEYS TO DEFENSIBLE POLICIES:**
 - POLICY CONTENTS
 - CONSISTENT ENFORCEMENT
- **Traditional concerns: physical conduct, whereabouts, etc.**
- **Modern added concerns: einfo; infosec; and Web 2.0:**
 - MANY more ways information can be lost or stolen
 - E-mail volume, persistence, “forwardability,” etc.
 - Now, MANY other forums; everyone can be a publisher
- **Hot topic**
 - See, e.g., Dubé, *ABA Panel Warns Employers to Act Carefully On Workplace Monitoring, Privacy Policies*, BNA PSLR (8/10/09), available by subscription at <http://ABA-BNA-PSLR-8-10-09.notlong.com>



I. The Modern Landscape –

B. Strange Things People Memorialize

- E-mails, Texting and IM, Oh My!
- CAN'T GO BACK IN TIME AND “TERMINATE” A WRITING . . . See, e.g., “*Nine Lives of E-mail*” (see Attached Appendix B)
- SO USE BEST EFFORTS TO REFRAIN FROM WRITING AND FROM OVER-SAVING
- ***Hot off the presses re: K-mart:***
 - ***“Hawkins is 64 yrs old with 20 yrs with km. I think I can get him to retire. Let me work on him.”***
 - ❖ ***Jason W. Armstrong, Mystery E-Mail Leads Del Mar Lawyers to Huge [\$26M] Verdict, New Niche (S.F. & L.A. Daily J. 8/27/09)***

I(B). 1. Damaging E-mails – “Jokes,” Affairs, etc.



- As described at <http://www.xbiz.com/news/88733?ht=all>:

“[C]ompare President Bill Clinton to a black man [because] Clinton played the saxophone, smoked marijuana and receives a check from the government each month”

- From <http://conservativebabylon.lavenderliberal.com/category/charles-a-rosenthal/>:



From: Rosenthal, Chuck
Sent: Tuesday, July 24, 2007 8:07 AM
To: Stevens, Kerry
Subject: RE:

I love you

From: Rosenthal, Chuck
Sent: Thursday, August 09, 2007 2:44 PM
To: Stevens, Kerry
Subject: RE: Me

*I always want to see you.
You own my heart whether you want or not*

From: Rosenthal, Chuck
Sent: Friday, August 10, 2007 6:06 PM
To: 'Kerry'
Subject: RE: RE:

The very next time I see you, I want to kiss you behind your right ear.

I(B)(1). Smoking Gun Activity *(c't'd)*— Cell-Phones/PDA's



- **Text messages string on employer-issued pagers:**
 - **Q: “And, did you miss me sexually?”**
 - **A: “Hell yeah!
You couldn’t tell.
I want some more.”**
 - ❖ **Detroit Mayor Kwame W. Kilpatrick (THEN a lawyer)**
 - ❖ **Long-time chief of staff, Christine Beatty (law student)**

**See articles linked: at footnote 25 at p. 6 of Paper;
and in list listed comprising Appendix H**

I(B). 2. Damaging Web Conduct *(c't'd)*—

a. Internet Activity



- **Another Mich. mayor story, from June 2009:**
 - **City check registry posted on web by Battle Creek mayor**
 - **Contained personally identifiable information on 65 city employees, including Soc. Sec. No for 6 of them**
 - **An employee had mistakenly given him the wrong item**
 - **Taken down quickly (within a day)**
 - **But employees offered free identity protection for 1 year**

See articles cited/linked in footnote 29 at p. 7 of Paper

I(B)(2). Internet Activity *(c't'd)* — b. Social Networking *(c't'd)*



- **Should elected officials be using Facebook, et al. to communicate with constituents?**
 - Risk/benefit analysis, per Maryland Legislature example
 - One of the risks: viruses, worms and malware . . .
 - See articles at footnote 331 at p. 76 of Paper
- ***But see***
 - Sabrina I. Pacifici, *House Committees Take the Lead on Using Social Media to Ensure Transparency*, beSpacific (3/2/09) <<http://www.bespacific.com/mt/archives/020728.html#020728>>
 - Twitter directory linked off of Slide 10 below

[FYI: FACEBOOK IS A FENWICK & WEST CLIENT]

I(B)(2)(b). Internet Activity *(c't'd)* – “Off-Duty” Postings



■ Current Employees’ Personal Postings

- Ian Shapira, *When Young Teachers Go Wild on the Web; Public Profiles Raise Questions of Propriety and Privacy*, Wash. Post (4/28/08) <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/27/AR2008042702213_pf.html>
- Michelle Yoffee-Beard, *Oviedo officer resigns after online sex ads, photos uncovered*, Seminole Chronicle (8/6/08) <www.seminolechronicle.com/vnews/display.v/ART/2008/08/06/489a38bf11c0e>

- TO LEARN MORE about a variety of related issues, see Ken Strutin, *Criminal Law Resources: Social Networking Online and Criminal Justice*, LLRX (2/28/09) <<http://www.llrx.com/node/2150/print>>

I(B)(2)(b). Web 2.0 Activity (c't'd) – Twittering . . .



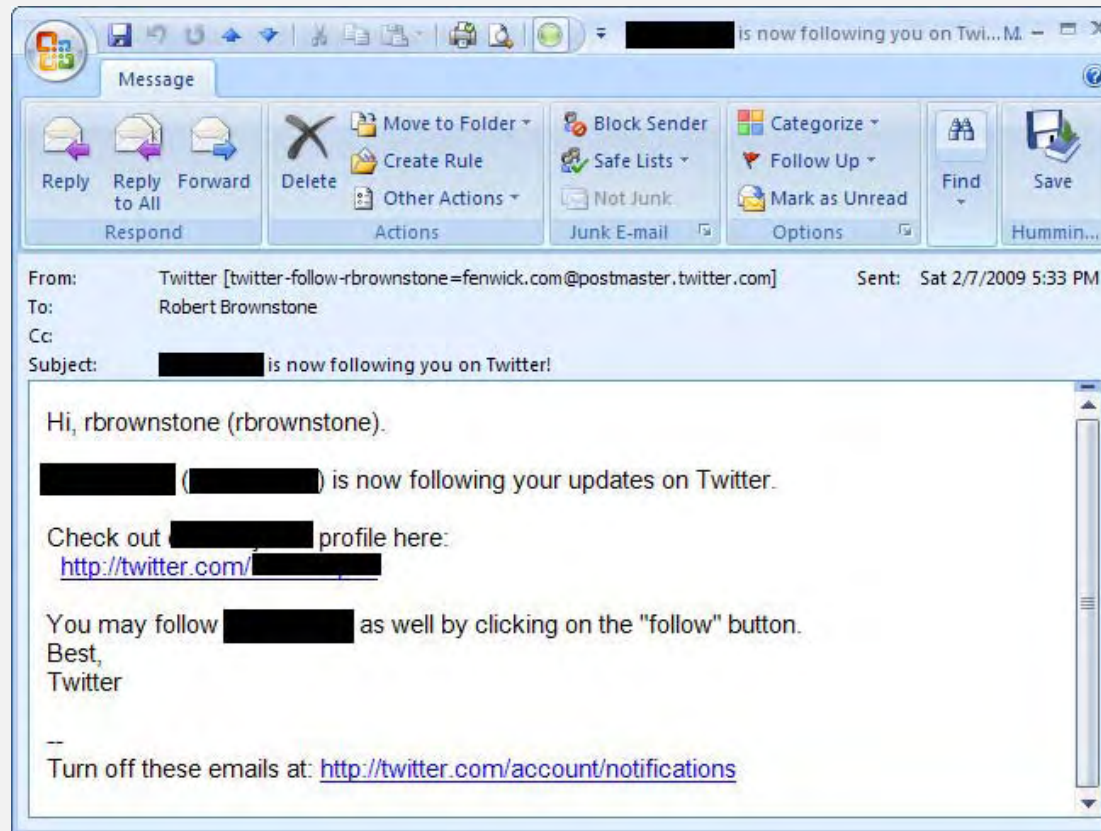
- From <http://twitter.com/petehoekstra/statuses/1182334669>:



- Rafe Needleman, *Congressman twitters secret trip to Iraq* (CNET news 2/6/09) http://news.cnet.com/8301-17939_109-10159054-2.html

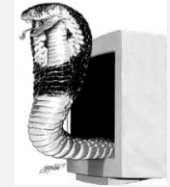
- See also <http://GovTwit.com>

I(B)(2)(b). Internet Activity (c't'd) — Twittering (c't'd) . . .



■ **See also:**

- **[President Obama's New Twitter Feed \(NYT 5/1/09\)](#)**
- **[Sports world chirping about Twitter to keep fans informed \(USA Today 4/28/09\)](#)**
- **[Giants closer also closes Twitter account \(USA Today 4/28/09\)](#)**



I(B)(2). c. Damaging Metadata and Embedded Data

- **MANY famous entities bitten
by cobra of embedded data**
- **Other Example: NELI ELB attendee**
- **Related Topic Ineffective
Electronic Redactions**
- **Many articles and press reports
*available on request from presenter***

I(B). 3. Internet Activity *(c't'd)* — Applicants' UGC



- *Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work*
- *Who is the hiring manager[?] I'm sure they [sic] would love to know that you will hate the work. We here at Cisco are versed in the web.*

Molly DiBianca, *Twitter Saves Cisco a Bundle of Money*, Del. Emp. Law Blog (3/30/09)

www.delawareemploymentlawblog.com/2009/03/twitter_saves_cisco_a_bundle_o.html

[<www.delawareemploymentlawblog.com> is a great resource]

**[FYI: COINCIDENTALLY, BOTH TWITTER AND
FACEBOOK ARE FENWICK & WEST CLIENTS]**



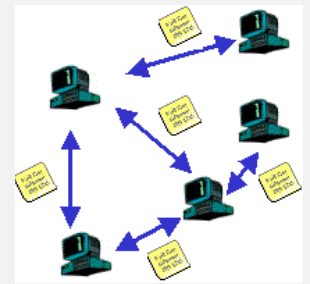
© Native Intelligence 2001

II. Monitoring Activity – A. Why Do So?

- **21st century employers have interests in preventing:**
 - Exposure of confidential information
 - Third parties' claims based on bad employee conduct (postings; copyright infringement via downloads, etc.)
 - Employees' harassment/discrimination claims
 - Basis for Computer Fraud & Abuse Act (CFAA) claim

- **Additional reasons to monitor:**
 - Network security (virus prevention, etc.)
 - Maintain and track productivity

II(A). Why Employers Monitor Electronic Activity *(c't'd)*



- **Justifications weighed against:**
 - risks, *e.g.*, mistrust, bad morale
 - employee privacy interests

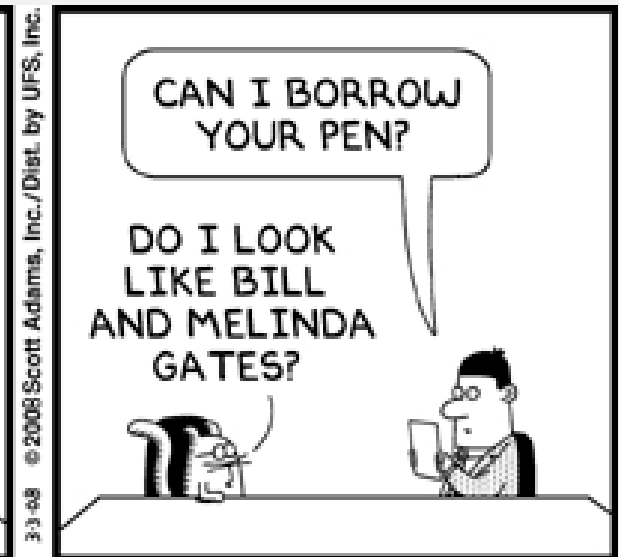


© Scott Adams, Inc./Dist. by UFS, Inc.



www.dilbert.com

scottadams@aol.com



©2008 Scott Adams, Inc./Dist. by UFS, Inc.

3-3-08

II. B. Monitoring's Legality – Statutory Highlights



- 1. **Electronic Communications Privacy Act (ECPA)**
 - **Wiretap Act (Title I):** forbids interception (data in transit)
 - **Stored Communications Act (SCA) (Title II):** prohibits access (data at rest and in storage)
- **ECPA exceptions include:**
 - **Wiretap Act & SCA “provider” definitions**
 - ❖ 18 U.S.C. § 2511(2)(a)(i), (h)(ii)
<<http://uscode.house.gov/download/pls/18C119.txt>>
 - ❖ 18 U.S.C. § 2701(c)
<<http://uscode.house.gov/download/pls/18C121.txt>>

II(B)(1). ECPA Redux



- **Same rules apply: in criminal and in civil cases; and to internet service providers (ISP's) and to employers**
- **Contract/policy language often becomes determinative**
- **Typically courts find employers acted within their rights *unless* examining locally-stored files impinges on an employee's attorney-client (a/c) privilege**

II(B)(1). ECPA – MOST RECENT KEY CIRCUIT DECISION



- ***Quon v. Arch Wireless* (9th Cir.):**
 - SCA violation for pager service provider to disclose City employee’s text messages to City/employer
 - 4th A. “expectation of privacy” violation: operational reality trumped old, unrevised policy language
- 529 F.3d 892 (9th Cir. 6/18/08) (“*Quon I*”)
<[www.ca9.uscourts.gov/ca9/newopinions.nsf/D2CDDDB4098D7AFB28825746C0048ED24/\\$file/0755282.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/D2CDDDB4098D7AFB28825746C0048ED24/$file/0755282.pdf?openelement)>
- See also denial of panel rehearing and of rehearing en banc, 2009 WL 224544, at *1-5 (1/27/09) (“*Quon II*”) <www.ca9.uscourts.gov/datastore/opinions/2009/02/06/0755282o.pdf>
But see dissent at 2009 WL 224544, at *6-11 (9th Cir. 1/27/09)
<<http://www.ca9.uscourts.gov/datastore/opinions/2009/02/06/0755282o.pdf#page=10>>
- **II(B). 2. State Analogues to the ECPA**
 - See pages 29-30 of Paper

II(B). 3. CFAA Justification For Monitoring



- **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”
 - “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)(4), (a)(5)(A)(i)

<http://uscode.house.gov/download/pls/18C47.txt>

- **See also Erika Morphy, *The Computer Fraud Act: Bending a Law to Fit a Notorious Case*, E-Commerce Times (12/09/08) (quoting me 😊)**
<http://www.ecommercetimes.com/story/65424.html#>



II(B)(3). CFAA Justification For Monitoring *(c't'd)*

■ Employers have had tenable CFAA claims where:

- Employee exceeded authorized access by, on eve of departure, transmitting trade secrets from work computer to home computer

Nilfisk-Advance v. Mitchell, 2006 WL 827073 (W.D. Ark. 3/28/06)

<https://ecf.arwd.uscourts.gov/cgi-bin/show_case_doc?13,26525,,,,52,1>

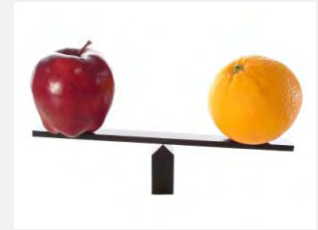
- Employee's laptop access rights terminated "when, having already engaged in misconduct and decided to quit . . . , he resolved to destroy files that . . . were . . . the property of his employer, in violation of the duty of loyalty"

Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 3/8/06)

<<http://caselaw.lp.findlaw.com/data2/circs/7th/051522p.pdf>>

- ### ■ For MANY other CFAA decisions going both ways (incl. 26 since 1/1/08), see pp. 30-38 of Paper

II(B). 4. Countervailing Concern # 1 – Union/Concerted-Activity



- **Recent Decision in *Guard Publ'ng Co. d/b/a Register-Guard v. NLRB*, 571 F.3d 53 (D.C. Cir. 7/7/09)**
<<http://pacer.cadc.uscourts.gov/common/opinions/200907/07-1528-1194980.pdf>>
 - Policy prohibited e-mail use “to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations”
 - Regional level upheld ULP charge based on reprimands for union-related e-mails
 - NLRB reversed in late 2007, espousing new standard (I call it “apples-to-apples”)
- **D.C. Circuit REVERSED, finding that the selective enforcement of e-mail policy’s no-solicitation rule unlawfully discriminatory**

II(B)(4). Union/Concerted-Activity – 2009 NLRA Decision *(c't'd)*



■ D.C. Cir. REASONING:

- One key e-mail was union-related but did not call for action; simply clarified facts as to a rally
- Other e-mails, though, were solicitations in that they did call for employees to take action to join union
- BUT those were the only co. e-mails ever prohibited
- Nor did disciplinary-warning invoke organization-vs.-individual line (apples-to-oranges) drawn by NLRB

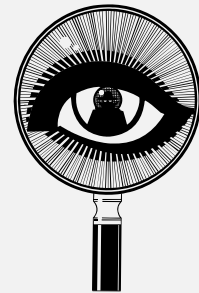
■ Takeaways?

- Avoid fine distinctions?
- Track rejections of personal use?
- ***Cf. Los Angeles County Superior Ct. (AFSCME Local 575) 24 (2008) PERB Dec. No. 1979-C, 32 PERC ¶ 151 (appeal pending)***



II(B). 5. Countervailing Concern # 2 – Invasion of Privacy Claims . . .

- For viable privacy claim – constitutional or common-law invasion – employee needs, key element: “**reasonable expectation of privacy**”
- Such claims usually not viable – due to legitimate employer interests and vitiating of employee’s privacy expectations
- Exceptional factual context – attorney-client privilege
 - As to split in decisions, see footnotes 96-98 at pp. 22-23 of Paper
- **TO LEARN MORE** about vitiating privacy contentions:
 - See articles at notes 168 & 170 (& accompanying text) at pp. 41-42 of Paper



III. Investigations & Background Checks

■ A. Credit Report Information

- FCRA/FACTA and State Analogues

- ❖ See pages 44-47 of Paper, including:

- notice of rights cited/linked in footnotes 191 & 192 at p. 45 of Paper;
- sample “FCRA DISCLOSURE FOR ADVERSE ACTION BASED ON NON-FACT ACT INVESTIGATIONS” at App. D-17; and
- set of sample forms in *Hiring Pa. Municipalities*, cited/ linked in footnotes 189 & 191 at p. 45 of Paper

- ❖ Important: FTC’s Disposal Rule under FACTA

III. Investigations & Background Checks



■ B. Legality & Advisability of Following Internet Trail on Prospective Employees

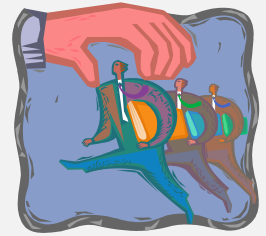
- Remember Cisco example
- “Drunken Pirate”: negatively evaluated Pennsylvania high school student-teacher’

❖ *Snyder v. Millersville University*, No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008)
<<https://ecf.paed.uscourts.gov/doc1/15304792325>>



III(B). Following the Internet Trail on Job Applicants

- **Legality and Advisability**
 - Those who post information about themselves on web without using protections to keep it from being publicly available have very weak “expectation of privacy” argument
 - ❖ See generally Jonathan Bick, *Lawful Mining of Blogs on Social Networks*, N.J.L.J. (2/19/09) (citing older caselaw) <www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428377614>
 - Employer may lawfully search/Google as to a prospect
 - ❖ *Mullins v. Dep’t of Commerce*, No. 06-3284, 244 Fed. Appx. 322, 2007 WL 1302152 (Fed. Cir. 5/4/07) <www.ll.georgetown.edu/FEDERAL/judicial/fed/opinions/06opinions/06-3284.pdf>



III(B). Following the Internet Trail on Job Applicants

- **Legality and Advisability** *(c't'd)*
 - As in “off-duty” context as to existing employees, if applicant’s posted content demonstrates lack of ability to do, or interest in, job, presumably no problem with prospective employer relying on it
 - The extent HR can use the found information in a hiring decision is subject to traditional labor law concepts such as discrimination

III(B). Following the Internet Trail on Job Applicants



- **Legality and Advisability** *(c't'd)*
 - What if, pre-interview, you learn of gender for, e.g., “Pat” or “Stacey” or “Hunter”?
 - OR, if pre- or post- interview, a social-networking page is only way hiring dep’t learns of a prospect’s:
 - ❖ religion
 - ❖ race
 - ❖ marital status
 - ❖ sexual preference

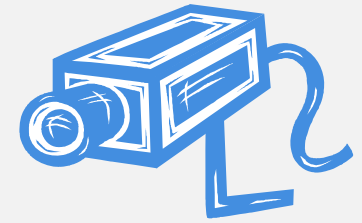
IV. Searching, Surveilling & Tracking Physical Conduct & Locations



■ A. Workplace & Personal Searches

- Reasonable expectations standard
- More complicated for public employers
 - ❖ *See Quon II* majority & dissent – heated debate as to *O’Connor v. Ortega*, 480 U.S. 709 (1987) (“**operational realities of the workplace may make some employees’ expectations of privacy unreasonable**”):
 - Dissent accused Majority of inaptly applying “less intrusive means” standard
 - Disagreement on whether search was “special needs” or “investigatory”
 - Interpretations varied of the factual record as to the breadth of uses to which officers supposed to put pagers

IV. Searching, Surveilling & Tracking Physical Conduct & Locations



■ B. Video Surveillance

- **Invasion-of-Privacy Concerns . . . From**

<http://dilbert.com/dyn/strip/000000000/00000000/0000000/000000/10000/3000/500/13538/13538.strip.gif>:



- **Very recent Cal. intrusion decision an anomaly?**

- ❖ *Hernandez v. Hillside, Inc.*, __ Cal. Rptr. 3d __, __ Cal. 4th __, 2009 WL 2356904 (Cal. 8/3/09)
www.courtinfo.ca.gov/opinions/documents/S147552.PDF



IV. Investigations & Background Checks

C. GPS Tracking – incl. RFID & GPS

- **Most employers not using**
 - More likely to track off-duty conduct
 - Risks of misinterpretation of data
 - Possible link to personally identifiable information (PII)
- **RFID (radio frequency ID systems) tags**
 - 4 states (Cal., Mo., N.D. & Wisc.) expressly prohibit compulsory implantation

IV. Investigations / Checks

D. “Off-Duty Activities

- 1. – 4. Competitive Business Activities; Substance Use; Dating and Intimate Relationships; Arrests and Convictions – See pages 56-62 of Paper
- Traditional concerns: competitive business activities; substance use if impacts job; dating and intimate relationships if prohibited by anti-fraternization policy and/or legal rules
 - **Ex: Delaware high school teacher’s termination upheld; immorality of affair with 17 year old he had taught when she in elementary school**
 - ❖ *Lehto v. Bd. of Ed. of Caesar Rodney School Dist.*, 962 A.2d 222 (Del. 2008)
<[http://courts.state.de.us/opinions/\(a4sdynji0why1t55z0gv2v45\)/download.aspx?ID=114560](http://courts.state.de.us/opinions/(a4sdynji0why1t55z0gv2v45)/download.aspx?ID=114560)>



IV. D. 5. “Off-Duty” Activities In Web Content

- Now . . . Miscellaneous Web Activities



- Keys if are going to discipline/terminate:
 - no reasonable expectation of privacy
 - nexus to job performance
 - consistent enforcement of “real” policy

IV(D)(5). “Off-Duty” Activities In Web Content *(c’t’d)*



■ Examples:

- **Resigned:** Iowa college president, after publication of above photo in newspaper
- **Fired:** Arizona police officer; 9th Cir. upheld dismissal based on website featuring sexually explicit photos & videos of wife
 - ❖ *Dible v. City of Chandler*, 515 F.3d 918, 924 (9th Cir. 2008)
<www.ca9.uscourts.gov/datastore/opinions/2008/01/31/0516577.pdf>
- **Fired:** Swiss insurance worker, whose at-home Facebook activity belied claim that, when on sick leave, could not use computer screen



IV(D)(5). “Off-Duty” Activities In Web Content *(c’t’d)*

■ EXAMPLES *(c’t’d)*

- **Suspended:** North Carolina facing possible termination for racially derogatory comments on her Facebook page:
 - ❖ Hobbies and activities: “drinking” and “teaching chitlins in the ghetto . . .”
 - ❖ "About Me": "teaching in the most ghetto school in Charlotte"
 - ❖ [4 other instructors also disciplined]

V. Implementing Compliant/ Legally-Defensible Policies



■ A. Introduction to Compliance

■ 1. Three E's: ■ Three-pronged approach

- **E**stablish ↔ Administration/Policies
- **E**ducate ↔ Training
- **E**nforce ↔ Technology

Let the Harmony Begin

TOSHIBA
Don't copy. Lead.®

© TOSHIBA

V(A)(1). Compliance Intro (c't'd) – 3 E's – Assess; THEN Draft

KUMBAYA – Legal, IT & HR and/or EO to Collaborate



V(A). Defensible Privacy Policies *(c't'd)*

2. Notice, Reasonableness, etc.



- Prophylactic agreements/policies can cut off future protracted litigation disputes
 - *Cf.* laptop/PC cases at footnotes 60, 311-12 and 325 in Paper
- KEY is to cover all *information* created, received or stored on: employer's network; or equipment provided ?or supported? ?or paid for? by employer
 - HOME PC?! *Cf.* MJD, Brett Favre might want to invest in his own cell phone, Yahoo Sports (7/23/08) <<http://Favre-Cell-7-23-08.notlong.com>>
- **MUST READ (though I do NOT think his suggested protocol is a magic bullet):** Peter Scheer, Commentary: Government officials use personal email and texting accounts to avoid public access laws. Why not use technology to enhance accountability instead of to subvert it? Cal. First Amendment Coalition (8/20/09) <www.cfac.org/content/index.php/cfac-news/commentary45/>

V(A)(2). Defensible Privacy Policies *(c't'd)* Reasonable Expectations *(c't'd)*



■ Specific Goals:

- Explicit employee consent to monitoring
- Clear notice of prohibited activities
 - ❖ reduce non-business-related activity
 - ❖ avoid liability

■ INTERNATIONAL CAVEAT

- Especially in EU
- ***But see new Finland law:***
 - ❖ <http://www.ioltechnology.co.za/article_print.php?iArticleId=4889373> (3/14/09)
 - ❖ <<http://news.theage.com.au/action/printArticle?id=405190>> (3/5/09)

V(B). Key Policies – Some Examples



- **Technology Use, incl. V-mail (Unified Messaging?)**
- **Banner/Flash-screen warnings?**
- **All company-issued mobile devices (laptops, PDA's, cell phones, etc.)**
- **Portable media (USB memory sticks, jump-drives, etc.)**
- **(Anti-) Blogging/Wikis**
- **Instant Messaging (IM) use or ban?**



V(B). Key Policies – Some Examples *(c't'd)*

- **Retention/Destruction Policy/Protocols**
 - incl. inspection/litigation provision
- **Separation Protocol & IT Checklist**
 - approval-process/workflow for:
 - ❖ over-writing (“re-imaging”) laptops (and other devices); and
 - ❖ emptying E-mail-box
- **Blogs/Web-2.0 Additions to existing policies? *E.g.:***
 - ❖ Internet/Technology-Use and/or Anti-Harassment Policies
 - ❖ As to Web 2.0, see samples linked from Jaffe article cited – with other Samples – in footnote 300 at p. 68 of Paper



V. C. Risks of Strict Policies – 1. Creation of Duty to Act?

- ***Reserving right to monitor versus taking on *duty* to monitor***
 - ***Ex. – Harassment***
 - ❖ Allocate resources (person-power) to follow through and review the electronic activity
 - ❖ Make sure to properly address inappropriate conduct
 - **Ex. – Other types of employee conduct?**
 - ❖ Potential liability to third party based on actual or constructive knowledge plus failure to remedy.
 - *Doe v. XYZ (N.J.)*



V(C). Risks of Strict Policies – 2. Prohibit Innocent Surfing?

- Probably better to be realistic in written policy (allowing incidental/limited personal uses)
- Otherwise, can be accused of arbitrary use of discretion in enforcement
 - *Cf.* ULP issue above
 - 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>>

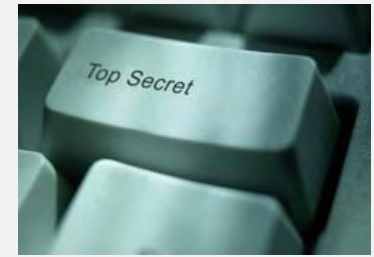
V. D. Periodic Training



- **Train new and veteran employees on above policies, plus these:**
 - **E-mail “Netiquette”**
 - **Attorney-Client Privilege**

- ***See Global Cisco Study Applies Reality Check to Corporate Security Policies, Draws Connection to Data Leakage Risk (10/28/08) <http://newsroom.cisco.com/dlls/2008/prod_102808.html>***
 - ***“Research Identifies **Gap in Policy Awareness of Employees**, Shows 1 in 4 Companies Lacks Security Policies”***

V. E. InfoSec Compliance – Resources/Frameworks



- Three major compliance frameworks . . .
ITIL . . . ISO 27002 (was 17799) . . . COBIT

- Ex. of flawed basic security measure: login
and password = e-mail-address + last-name

Andrew Clevenger, *Lawyer admits computer breach; [s]pying on firm may cost license*, Charleston Gazette (3/2/08) <<http://sundaygazette.com/News/200803010561>>

Lawyers Disciplinary Bd. v. Markins, No. 33256 (W. Va. Sup. Ct. App. 5/23/08) <<http://www.state.wv.us/WVSCA/docs/Spring08/33256.pdf>>

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





Conclusion/ Questions

■ Q+A

- Robert D. Brownstone

- ❖ <www.fenwick.com/attorneys/4.2.1.asp?aid=544>
- ❖ 650.335.7912 or <rbrownstone@fenwick.com>



■ Please visit F&W EIM

- ❖ <www.fenwick.com/services/2.23.0.asp?s=1055>
- ❖ <www.fenwick.com/services/2.23.4.asp?s=1055>

■ See also F&W Privacy & EMP Groups

- ❖ <<http://www.fenwick.com/services/2.14.0.asp?s=1045>>
- ❖ <<http://www.fenwick.com/services/2.7.0.asp?s=1041>>

APPENDIX B

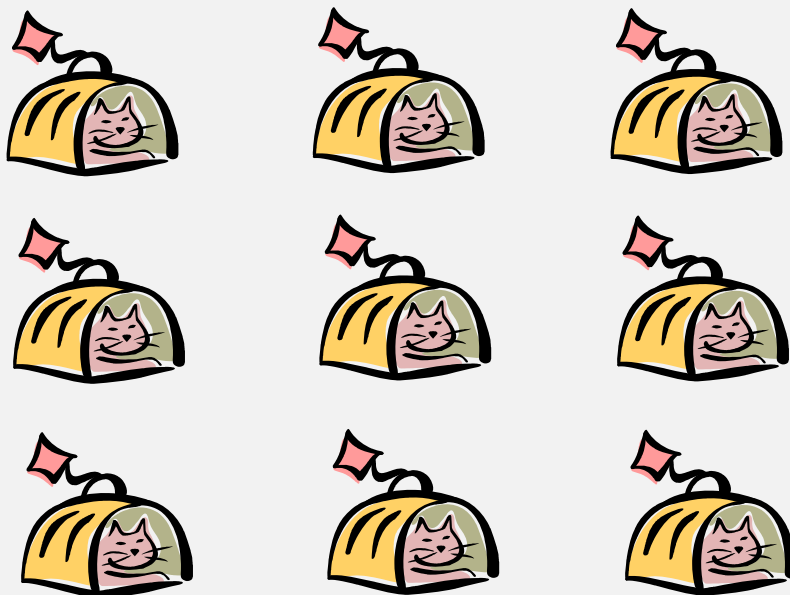
*For NELI
Public-Sector/
EEO Attendees
August 28, 2009*

© FENWICK & WEST LLP



E-mail's Nine Lives

© 2007, 2008, 2009



Robert D. Brownstone, Esq.

Fenwick & West LLP

E-mail's Nine Lives? – Never “Terminated”?



*"Quick, delete that e-mail
before Eliot Spitzer sees it!"
(Corante NY 7/29/05)*

- **Live/Active**
 - 1. Central server or e-mail database
 - 2. Sender's or Recipient's Mailbox OR Hard Drive
 - 3. Other Recipient's (FW, CC, BCC) Mailbox OR Hard Drive
 - 4. Sender's or Recipient's PDA OR DVD OR CD
 - 5. If Webmail (Google, Yahoo) and recent . . . Temporary Internet File
- **Relatively Inaccessible (“not reasonably accessible”)**
 - 6. Back-up tapes of sender's employer or ISP
 - 7. Back-up tapes of recipient's employer or ISP
 - 8. Back-up tapes of another recipient's employer or ISP
 - 9. Forensically recoverable “deleted” message or fragment
- **CAN'T GO BACK IN TIME AND “TERMINATE” IT**
- **SO USE BEST EFFORTS TO REFRAIN
FROM WRITING AND FROM OVER-SAVING**

Conclusion/ Questions



■ Q+A

- Robert D. Brownstone

- ❖ www.fenwick.com/attorneys/4.2.1.asp?aid=544
- ❖ 650.335.7912 or rbrownstone@fenwick.com



■ Please visit F&W EIM

- ❖ www.fenwick.com/services/2.23.0.asp?s=1055
- ❖ www.fenwick.com/services/2.23.4.asp?s=1055

■ See also F&W Privacy & EMP Groups

- ❖ <http://www.fenwick.com/services/2.14.0.asp?s=1045>
- ❖ <http://www.fenwick.com/services/2.7.0.asp?s=1041>

APPENDIX C

SAMPLE SUMMARY/ROLL-OUT MEMO REGARDING TECHNOLOGY ACCEPTABLE USE AND LACK-OF-EMPLOYEE-PRIVACY POLICY

[at times integrated with summary of Records-Retention Policy]

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH.

LEGAL OBLIGATIONS DIFFER AMONG: U.S. JURISDICTIONS; DIFFERENT COUNTRIES; AND INDUSTRIES. TECHNOLOGY AND WORKPLACE CIRCUMSTANCES ALSO VARY GREATLY.

THUS, THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE.

ANYONE WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

TECHNOLOGY ACCEPTABLE USE POLICY – HIGHLIGHTS

Introduction

In the next **[number]** weeks, we will be issuing **[a revised version of]** a key policy: **[Company's]** Technology Acceptable Use [and Lack of Employee Privacy] Policy (the "AUP Policy"). The AUP policy is designed to help you understand the acceptable uses of **[Company]** resources.

This memo is a brief outline of the AUP Policy and a reminder to comply with **Company** requirements and legal guidelines as to information security and information management.

Please read and review the full AUP Policy, which contain a more detailed description of employees' obligations. Please also attend the upcoming "Net-iquette" training.

I. Incidental Personal Use:

[Company] provides information technology resources for business purposes. Limited personal use is allowed *only* if it does not interfere with your job duties, aim to generate personal financial gain, conflict with **[Company]**'s business interests or violate the law or any **[Company]** policy.

II. Forbidden Uses

Use of **[Company]**'s information technology systems, networks and equipment is a privilege, not a right. Employees must not: engage in illegal or inappropriate conduct; transmit statements derogatory or threatening toward any person or group; violate **[Company]**'s **Policy Against Discrimination or Harassment [make sure it exists and name is correct]**; or download, copy or install unlicensed software, music, video or other media. For specific license questions, contact our **Information Technology Department [make sure it exists and name is correct]**

III. No Expectation of Privacy **[REMEMBER: DIFFERENT APPROACH NEEDED IN EU]**

All information created, sent, received and stored on any **[Company]** system or device is **[Company]**'s property. Therefore, employees should not have any expectation of privacy as to any such information. The **[Company]** reserves the right, at any time, in its sole discretion, to monitor, search, access and read all such information – including all email and voicemail messages.

As a result, employees should use discretion and good judgment before using **[Company]** property for personal use and should assume that, once created, any "personal" content will not be confidential.

APPENDIX D

SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 1

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH.

LEGAL OBLIGATIONS DIFFER AMONG U.S. JURISDICTIONS, AMONG DIFFERENT COUNTRIES AND AMONG INDUSTRIES. TECHNOLOGY AND WORKPLACE CIRCUMSTANCES ALSO VARY GREATLY.

THUS, THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

I. General Provisions

A. Introduction

The Company provides various Technology Resources to authorized employees to assist them in performing their job duties for the Company. Each employee has a responsibility to use the Company's Technology Resources in a manner that increases productivity, enhances the Company's public image, and is respectful of other employees. Failure to follow the Company's policies regarding its Technology Resources may lead to disciplinary measures, up to and including termination of employment.

B. Technology Resources Definition

Technology Resources consist of all electronic devices, software, and means of electronic communication, including, but not limited to, the following, whether provided or supported by the Company: personal computers and workstations; laptop computers; mini and mainframe computers; computer hardware such as disk drives and tape drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet; electronic mail; telephones; cellular phones; pagers; and voicemail systems.

C. Authorization

Access to the Company's Technology Resources is within the sole discretion of the Company. Generally, employees are given access to the Company's various technologies based on their job functions. Only employees whose job performance will benefit from the use of the Company's Technology Resources will be given access to the necessary technology.

D. Use

The Company's Technology Resources are to be used by employees only for the purpose of conducting Company business. Employees may, however, use the Company's Technology Resources for the following incidental personal uses so long as such use does not interfere with the employee's duties, is not done for pecuniary gain, does not conflict with the Company's business, and does not violate any Company policy:

- (1) To send and receive necessary and occasional personal communications;
- (2) To prepare and store incidental personal data (such as personal calendars, personal address lists, and similar incidental personal data) in a reasonable manner;
- (3) To use the telephone system for brief and necessary personal calls; and
- (4) To access the Internet for brief personal searches and inquiries during meal times or other breaks, or outside of work hours, provided that employees adhere to all other usage policies. [OPTIONAL ADDITIONAL SENTENCE: The Company acknowledges that employees may, at other times, engage in incidental personal use of the Internet, as long as such use does not interfere with the performance of job duties.]

The Company assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on the Company's Technology Resources. The Company accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on any Company property. The Company strongly discourages employees from storing any personal data on any of the Company's Technology Resources.

II. Improper Uses

A. Prohibition Against Harassing, Discriminatory and Defamatory Use

The Company is aware that employees use electronic mail for correspondence that is less formal than written memoranda. Employees must take care, however, not to let informality degenerate into improper use. As set forth more fully in the Company's "Policy Against Harassment," the Company does not tolerate discrimination or harassment based on gender, pregnancy, childbirth (or related medical conditions), race, color, religion, national origin, ancestry, age, physical disability, mental disability, medical condition, marital status, sexual orientation, family care or medical leave status, veteran status, or any other status protected by state and federal laws. Under no circumstances may employees use the Company's Technology Resources to transmit, receive, or store any information that is discriminatory, harassing, or defamatory in any way (e.g., sexually-explicit or racial messages, jokes, cartoons).

B. Prohibition Against Violating Copyright Laws

Employees must not use the Company's Technology Resources to copy, retrieve, forward or send copyrighted materials unless the employee has the author's permission or is accessing a single copy only for the employee's reference.

C. Other Prohibited Uses

Employees may not use any of the Company's Technology Resources for any illegal purpose, violation of any Company policy, in a manner contrary to the best interests of the Company, in any way that discloses confidential or proprietary information of the Company or third parties, or for personal or pecuniary gain.

III. Company Access To Technology Resources

A. Introduction

All messages sent and received, including personal messages, and all data and information stored on the Company's electronic-mail system, voicemail system or other computer systems/resources are Company property regardless of the content. As such, the Company reserves the right to access all of its Technology Resources including its computers, voicemail and electronic-mail systems, at any time, in its sole discretion.

B. Lack of Privacy

Although the Company does not wish to examine personal information of its employees, on occasion the Company may need to access any and all information in its Technology Resources, including computer files, electronic-mail messages, and voicemail messages.

Employees should understand, therefore, that they have no right of privacy with respect to any information or messages – including personal information or messages – created, received or maintained on the Company's Technology Resources. The Company may, at its discretion, inspect all files or messages on its Technology Resources at any time for any reason.

The Company may also monitor its Technology Resources at any time to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

C. Passwords

Certain of the Company's Technology Resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. Passwords do not confer any right of privacy upon any employee of the Company. Thus, even though employees may maintain passwords for accessing Technology Resources, employees must not expect that any information maintained on Technology Resources, including electronic-mail and voicemail messages, is private. Employees are expected to maintain their passwords as confidential.

Employees must not share passwords and must not access coworkers' systems without express authorization.

D. Data Collection

The best way to guarantee the privacy of personal information is not to store or transmit it on the Company's Technology Resources. To ensure that employees understand the extent to which information is collected and stored, below are examples of information currently maintained by the Company. The Company may, however, in its sole discretion, and at any time, alter the amount and type of information that it retains.

- (1) Telephone Use and Voicemail: Records are kept of all calls made from and to a given telephone extension. Although voicemail is password protected, an authorized administrator can reset the password and listen to voicemail messages.
- (2) Electronic Mail: Electronic mail is backed-up and archived. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail.
- (3) Desktop Facsimile Use: Copies of all facsimile transmissions sent and received are maintained in the facsimile server.
- (4) Document Use: Each document stored on Company computers has a history, which shows which users have accessed the document for any purpose.
- (5) Internet Use: Internet sites visited, the number of times visited, and the total time connected to each site is recorded and periodically monitored.

E. Deleted Information

Deleting or erasing information, documents, or messages maintained on the Company's Technology Resources is, in most cases, ineffective. All employees should understand that any information kept on the Company's Technology Resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee. Because the Company periodically backs-up all files and messages, and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.

IV. Internet and Electronic Mail Policy

A. Proper and Improper Uses

The Company provides employees with access to the Internet and electronic mail to assist them in conducting the Company's business. The Company expects that when employees use the Internet or electronic mail during work hours, while on the Company's premises, or remotely through the use of the Company computer equipment, they will do so in a responsible manner, and for work-related purposes only. [OPTIONAL ADDITIONAL SENTENCE: The Company acknowledges that employees may, at other times, engage in incidental personal use of the Internet, as long as such use does not interfere with the performance of job duties.]

The Company expects employees to exercise discretion and good judgment when accessing the Internet, or when sending or receiving electronic mail and attachments thereto.

Improper use of the Internet and electronic mail includes, but is not limited to, the following:

- Use which is illegal, which is contrary to the Company's best interests, or which violates or conflicts with the Company's policies, including, but not limited to, the Company's policies against discrimination or harassment.
- Use, which discloses or leads to the disclosure of confidential or proprietary information about the Company.
- Use of electronic mail, chat rooms or other Internet devices that is defamatory or offensive in any way, including, but not limited to, racially or sexually charged messages, jokes or cartoons.
- Use of Internet sites, which may damage or interfere with the Company's computer network, including use that generates the delivery of "junk" electronic mail.
- Use that violates copyright laws.
- Personal use, and/or use which is not work-related.

Improper use of the Internet or electronic mail may lead to discipline, including, but not limited to, discharge from employment.

Employees have no right of privacy, nor any expectation of privacy, with respect to any aspect of their use of the Internet or electronic mail while on the Company's premises, or when accessing the Internet or using electronic mail remotely. The Company reserves the right to, at any time, without limitation, monitor your use of the Internet, including monitoring Internet sites visited, the number of times those sites are visited, and the time connected to each site.

All items uploaded to or downloaded from any location on the Internet, and all electronic mail and attachments thereto, must be scanned for viruses. Materials downloaded from the Internet must be placed on diskettes, and not on your computer hard drive, or the Company's network. Employees must use anti-virus software to scan any material from obtained via the Internet. Files or documents sent outside of the Company via the Internet and/or electronic mail must be properly encrypted. For any questions about encryption, or other protective measures you may employ in using the Internet or electronic mail, please contact the Human Resources Department or the Information Technology Department.

B. Confidentiality

Some of the information to which the Company has access is confidential. Employees should avoid sending confidential information over the Internet, except when absolutely necessary. Employees also should verify electronic mail addresses before transmitting any messages.

C. Monitoring

The Company monitors both the amount of time spent using on-line services and the sites visited by individual employees. The Company reserves the right to limit such access by any means available to it, including revoking access altogether.

V. Software Use

A. License Restrictions

All software in use on the Company's Technology Resources is officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the Company's computers, by any means of transmission, unless authorized in writing in advance by _____ [*specify, e.g., Technology Coordinator, Office Manager, etc.*]. Authorization for loading software onto the Company's computers should not be given until the software to be loaded has been thoroughly scanned for viruses.

B. Confidential Information

The Company is very sensitive to the issue of protection of trade secrets and other confidential and proprietary information of both the Company and third parties ("Confidential Information"). Therefore, employees are expected to use good judgment and to adhere to the highest ethical standards when using or transmitting Confidential Information on the Company's Technology Resources.

Confidential Information should not be accessed through the Company's Technology Resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended.

SAMPLE TECHNOLOGY USE AND LACK-OF-PRIVACY POLICY 2

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH.

LEGAL OBLIGATIONS DIFFER AMONG U.S. JURISDICTIONS, AMONG DIFFERENT COUNTRIES AND AMONG INDUSTRIES. TECHNOLOGY AND WORKPLACE CIRCUMSTANCES ALSO VARY GREATLY.

THUS, THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

I. Introduction

The Company allows employees to use company-owned computers and have access to the Company's network, email, the Internet, and telephone/voice mail/call log systems (collectively referred to as "Electronic Communications"). Such use encompasses, computers, laptops and other mobile devices, whether provided or supported by the Company (collectively referred to as "Company equipment"). Employees are responsible for ensuring that their use of the Company's Electronic Communications is professional, courteous, does not violate any laws, and maintains the security of the Company's confidential information.

The purpose of this policy is to: (1) notify employees that Electronic Communications are not private or confidential within the Company; (2) educate Employees on how to protect the Company's Trade Secrets stored electronically; and (3) educate Employees on the appropriate use of Electronic Communications.

II. Company's Access, Review, Deletion and Disclosure of Electronic Communications

The Company's Electronic Communications systems are for business use. The Company has the technical capability to access, review, copy, modify and delete any Electronic Communications transmitted through or stored on Company equipment or on the Company's network. The Company reserves the right to monitor, access, review, copy, disclose, modify or delete all such Electronic Communications at any time. All Electronic Communications are the property of the Company. Examples of common situations where the Company might access or monitor Electronic Communications are:

- System maintenance;
- Quality control and performance assessment, such as for Call Center activities;
- Internal investigation of wrongdoing, such as trade secret theft;
- The unexpected absence or termination of an employee who regularly receives business related email may require his or her manager to log into his or her email or voicemail to review such messages;

- To investigate sexual or other forms of harassment, or violation of the Company's policies;
- Investigations by governmental agencies;
- Court orders.

Be aware that even if you have deleted an email message, the message still exists if the network has been backed up prior to your deleting the message. Employees should be aware that Electronic Communications created, received or stored on the Company's equipment or the network may not remain private. Employees should treat the network like a shared file system - with the expectation that files sent, received or stored anywhere in the network, as well as the Company sites viewed by Employees, will be available for review by any authorized representative of the Company.

III. Protecting the Company's Confidential Information

You must exercise the same degree of caution (if not more) in transmitting the Company's confidential information on the email system that you take with other means of communicating information, (e.g., written memoranda, letters or phone calls) because of the ease with which such information can be further transmitted. Exercise care when using distribution lists to ensure that all addressees are appropriate recipients of the information. Lists are not always kept current and individuals using lists should take measures to ensure that the lists are current. International Electronic Communications may be monitored by local governments. Therefore, employees should exercise special caution before sending any sensitive Electronic Communications to foreign countries. Employees are also responsible for following all other policies regarding the Company's customer confidential information.

IV. Attorney-Client Privileged Communications

Some of the email messages or memoranda sent, received or stored on the Company's equipment or the network may constitute confidential, privileged communications between the company and its attorneys (whether in-house or outside). Upon receipt of a privileged or confidential message or memorandum either from or to counsel, do not forward it or its contents to others inside or outside the company without first speaking to counsel. When sending a confidential email to the company's attorneys, write in the subject or text of the email "Attorney-Client Communications."

V. Appropriate Use of Electronic Communications

The Electronic Communication systems are provided to employees, at the Company's expense, for their use on Company business. While occasional personal use of the computers, email system and telephone/voicemail is permitted if it does not interfere with timely work performance, all Electronic Communications, whether internal or external, and all use of the Company's equipment and the network, including Internet access, should be conducted in a professional manner. The Company uses content filtering software to protect users from harmful, unwanted and offensive messages. The software has been tuned to filter out most of the

undesired mail without trapping any business related messages. However, if you use the Company's mail system for personal messages, some messages may also be deleted though they may not be harmful, unwanted or offensive. If it is important for you to receive these messages, we recommend using a personal account.

Employees may not use the Company's Electronic Communications to engage in communications that are in violation of Company policy. The following are examples of inappropriate use of the Company's Electronic Communications systems: (1) transmitting or posting defamatory, obscene, offensive, threatening or harassing messages on servers or electronic bulletin boards or by voice mail; (2) copying or transmitting software or other information protected by copyright without an appropriate license; (3) accessing another employee's or contractor's email or voicemail without authorization; (4) downloading offensive material off the Internet; (5) sending chain letters; (6) offering weapons for sale via Public Folders (Classified Ads).

Keep in mind that the content of email messages sent over the Internet reflects on the Company. For example, if an employee sends a hostile or insulting email about a Company business partner to an individual over the Internet or posts such to an Internet bulletin board, the message could be perceived as reflecting the official Company viewpoint, which could interfere with the Company's business dealings and impair the Company's reputation. Defamatory messages could also lead to legal liability for both the employee and the Company.

Employees should be aware that the Company has the ability and the right to review the types of Internet sites accessed through its Electronic Communications systems, and should govern their access accordingly.

Violation of this Electronic Communications policy may result in discipline, up to and including termination of employment.

SAMPLE ELECTRONIC MAIL POLICY

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH.

LEGAL OBLIGATIONS DIFFER AMONG U.S. JURISDICTIONS, AMONG DIFFERENT COUNTRIES AND AMONG INDUSTRIES. TECHNOLOGY AND WORKPLACE CIRCUMSTANCES ALSO VARY GREATLY.

THUS, THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

I. Introduction

This policy sets forth the Company's policies with regard to access to, review, or disclosure of electronic mail ("email") messages sent or received by Company employees with the use of the Company's email system.

This policy also sets forth requirements as to the proper use of the email system.

[THESE NEXT TWO PARAGRAPHS TO BE ALTERED DEPENDING ON COMPANY'S IT ENVIRONMENT AND DESIRED APPROACH TO COMPANY-SUPPORTED EQUIPMENT]

This policy applies in equal force to all of the following ways of using the Company's e-mail system: when physically on Company premises and logged into the network, when accessing the e-mail system remotely via Virtual Private Network and over the internet via a web browser (i.e., Outlook Web access).

This policy applies in equal force to all types of equipment – whether provided or supported by the Company – that could be used to access the Company's e-mail system, including personal computers, laptop computers and PDA's and other mobile devices.

II. Use For Business Purposes/Company Access, Review, Deletion And Disclosure

The email system is provided to employees at the Company's expense to assist them in carrying out Company business. The email system permits employees to communicate with each other internally and with selected outside individuals and companies that the Company, in its sole discretion, decides should be connected to the system.

The email system is to be used for business related purposes only to transmit business information. [OPTIONAL ADDITIONAL SENTENCE: The Company acknowledges that employees may, at other times, engage in incidental personal use of the e-mail system, as long as such use does not interfere with the performance of job duties.] In any event, the Company treats all messages sent, received or stored in the email system as business messages.

The Company has the capability to access, review, copy and delete any messages sent, received or stored on the email system. The Company reserves the right to access, review, copy

or delete all such messages for any purpose and to disclose them to any party (inside or outside the Company) it deems appropriate.

Should employees make incidental use of the email system to transmit personal messages, such messages will be treated no differently from other messages, i.e., the Company reserves the right to access, review, copy, delete or disclose them for any purpose. Accordingly, employees should not use the email system to send, receive or store any messages that they wish to keep private. Users should treat the email system like a shared file system - with the expectation that messages sent, received or stored in the system (including individual hard disks) will be available for review by any authorized representative of the Company for any purpose.

III. Confidential Information

Essentially, email messages should be treated in the same way as confidential printed materials. There are three common circumstances where confidentiality can be breached:

- You leave the email program running on your screen, or leave an email message on your screen. In either case, this allows others to view your email should they sit at your computer.
- A confidential message is printed on a printer in your office or perhaps on a shared printer down the hall. Anyone with access to that printer can view this document.
- An email message is inadvertently sent to someone who was not intended to receive it. Caution should be exercised on any confidential messages before it is sent.
- Caution should be used when using the Internet. The Internet is a nice, cheap way to send business communications that aren't a security risk or time sensitive. Do not rely on the Internet for critical communications due to the possibility of compromise.

Users must exercise a greater degree of caution in transmitting confidential information on the email system than they take with other means of communicating information, (e.g., written memoranda, letters or phone calls) because of the reduced human effort required to redistribute such information. Confidential information should never be transmitted or forwarded to outside individuals or companies not expressly authorized to receive that information and should not even be sent or forwarded to other users inside the Company who do not need to know the information. Always use care in addressing email messages to make sure that messages are not inadvertently sent to outsiders or the wrong person inside the Company. In particular, exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information. Lists are not always kept current and individuals using lists should take measures to ensure that the lists are current. Refrain from routinely forwarding messages containing confidential information to multiple parties unless there is a clear business need to do so.

IV. Email Security

The security on our email system is as good as password security can be. If your network and email passwords are easy to discover, then your email can easily be accessed by anyone with that intention. It is strongly advised that you not use your first or last name, the Company name or other such passwords. It is also advisable to change your password periodically.

V. Viewing and Protecting Emails

In order to further guard against dissemination of confidential information, users should not access their email messages for the first time in the presence of others. Email windows should not be left open on the screen when the computer is unattended. Email passwords (as well as other computer passwords) should be routinely changed every three to four weeks.

VI. Copyrighted Information

Use of the email system to copy and/or transmit any documents, software, or other information protected by the copyright laws is prohibited.

VII. Email Etiquette

Please bear in mind that your email messages may be read by someone other than the addressee you send them to and may even someday have to be disclosed to outside parties or a court in connection with a litigation. Accordingly, please take care to ensure that your messages are courteous, professional and businesslike.

VIII. Other Prohibited Uses

Use of the email system to engage in any communications that are in violation of Company policies, including but not limited to transmission of defamatory, obscene, offensive or harassing messages, or messages that disclose personal information about other individuals without authorization, is prohibited.

Employees should promptly report any violations of this policy to the Company's HR or IT department.

IX. Storing and Deleting Email Messages

[SHOULD BE ALTERED SO CONTENT SYNCHS WITH
CONTENT OF COMPANY'S RETENTION POLICY]

The Company strongly discourages the storage of large numbers of email messages for a number of reasons. First, because email messages frequently contain confidential information, it is desirable to limit the number, distribution and availability of such messages to protect the Company's information. Second, retention of messages fills up large amounts of storage space on the network server and personal hard disks, and can slow down the performance of both the network and individual personal computers. Finally, in the event that the Company needs to search the network server, backup tapes, or individual hard disks for genuinely important

documents, the fewer documents it has to search through, the more economical the search will be.

Accordingly, employees are to promptly delete any email messages they send or receive that no longer require action or are not necessary to an ongoing project.

SAMPLE ACKNOWLEDGMENT OF RECEIPT

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH.

LEGAL OBLIGATIONS DIFFER AMONG U.S. JURISDICTIONS, AMONG DIFFERENT COUNTRIES AND AMONG INDUSTRIES. TECHNOLOGY AND WORKPLACE CIRCUMSTANCES ALSO VARY GREATLY.

THUS, THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

I acknowledge that I have received and read the foregoing Technology Acceptable Use and Lack-of-Employee Privacy Policy. I agree that I will follow the rules, guidelines and restrictions set forth in these policies.

I understand that the Company may modify, add to, delete or revoke any and all policies, procedures, practices, and statements contained in these policies at any time without prior notice to me. Such changes shall be effective immediately upon approval by management unless otherwise stated.

I understand that these policies are not intended to be a contract (express or implied), nor are they intended to create, nor do they create, any legally enforceable obligation on the part of the Company or its employees.

Signed: _____

Print Name: _____

Date: _____

NOTE TO THE EMPLOYEE: The original of this form will go into your personnel file. The Human Resource Department will send a copy of the form to you. **[WORDING SHOULD DIFFER IF ORGANIZATION FOLLOWS A PAPERLESS/AUTOMATED WORKFLOW]**

SAMPLE BLOGGING POLICY

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH.

LEGAL OBLIGATIONS DIFFER AMONG U.S. JURISDICTIONS, AMONG DIFFERENT COUNTRIES AND AMONG INDUSTRIES. TECHNOLOGY AND WORKPLACE CIRCUMSTANCES ALSO VARY GREATLY.

THUS, THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

[SHOULD BE MODERNIZED BY ADDRESSING SOCIAL-NETWORKING SITES, ETC.]

The Company understands that some employees may wish to create and maintain personal Web logs or “blogs.” While the Company respects your right to personal expression and views your blog as your personal project, you must also understand that your personal blog can impact the Company. Therefore, we ask that you follow these guidelines when posting to your personal blog.

Personal Expression. Personal blogs contain the views of a particular employee, not the Company; however, readers may not immediately appreciate this concept. If you choose to discuss your employment or identify yourself as a Company employee in any way, you should include a disclaimer that the views expressed do not necessarily reflect the views of the Company.

Protect Confidential/Trade Secret Information. As more fully described in the Company’s Confidential Information Policy and your Employee Confidential Information and Invention Assignment Agreement (“Agreement”), you should refrain from disclosing confidential, proprietary, sensitive and/or trade secret information of the Company and third-parties. Such disclosures threaten the Company’s intellectual property rights, ongoing business with third parties, and compliance with all securities laws. Additionally, the Company may have certain rights in any inventions or concepts you create that relate to the Company’s business; you should consult your manager and your Agreement before disclosing such inventions or concepts in your blog.

Be Respectful and Exercise Common Sense. Harassment of other employees will not be tolerated. Blogs should not violate the Company’s conduct-related policies, including its Code of Conduct, Equal Employment Opportunity, and Anti-Harassment Policies. When posting to your blog, be respectful of others. Assume that people, including co-workers and customers, are reading your blog. Even after you delete your blog, certain technology may still make that content available to readers.

Company Time and Company Equipment. The Company's Internet and Computer Use Policy governs all uses of Company computer equipment. Consult that policy before using Company equipment or time to create or update your blog. Further, as described in that policy, the Company reserves the right to monitor use of Company computer equipment.

The Company, in its sole discretion, will determine whether a particular blog violates Company policies. As with all other policies, violation of this policy may result in discipline, up to and including termination. The Company further reserves the right to request employees refrain from commenting on topics related to the company (or, if necessary, suspend the blog altogether), if advisable to comply with securities or other laws. Should you have any questions about this policy or how it may apply to your blog, please contact the Human Resources Manager.

**SAMPLE FCRA DISCLOSURE FOR ADVERSE ACTION
BASED ON NON-FACT ACT INVESTIGATIONS**

THIS SAMPLE REFLECTS ONLY ONE GENERIC APPROACH. THE CONTENTS OF THIS SAMPLE ARE NOT TO BE REGARDED AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS WITH PARTICULAR QUESTIONS SHOULD SEEK ADVICE OF COUNSEL.

[See generally FTC, *Using Consumer Reports: What Employers Need to Know* (Mar. 1999) <<http://www.ftc.gov/bcp/edu/pubs/business/credit/bus08.shtm>>]

Date
Name of Applicant/Employee
Address

Dear – [Name of applicant/employee] --:

We previously informed you that we would advise you of any employment action taken based in whole or in part on the information contained in the background investigation report we obtained on you. At that time, you were also provided a copy of that report.

– [Explanation of adverse action – refusal to hire, promote, reassign or continue employment.] –

Our decision was based wholly or in part on information contained in the report issued by:

- – [Name of CRA] –
- – [Address] –
- – [Telephone number (include a toll-free number if a nationwide CRA)] –

[CRA] – did not make a decision to – [describe action] – and is not able to explain to you why the decision was made.

You have the right under the Fair Credit Reporting Act to obtain a free copy of the report from – [CRA] – if you make a written request directly to – [CRA] – within sixty (60) days of your receipt of this notice. You have the right to directly dispute with – [CRA] – the accuracy or completeness of any of the information contained in the report.

Any inquiry concerning your report or any information contained therein should be directed to – [CRA] –. Please refer to the enclosed *Summary of Your Rights Under The Fair Credit Reporting Act* <www.ftc.gov/os/2004/07/040709fcraappxf.pdf>.

Date: _____

Signature for Employer

Typed Name and Title

Robert D. Brownstone – Information Law & Technology – Bibliography (8/7/09)

Publications

- *How to Protect Your Clients' and Your Firm's Electronic Information*, 30 The Bottom Line No. 4, at 1 (Aug. 2008) <http://members.calbar.ca.gov/sections/lpmt/bottomline/pdfs/the-bottom-line_2009_vol-30_no-4.pdf> (Cal. State Bar LPMT Section membership required to use URL; copy available from author)
- *California eDiscovery Legislation Signed Into Law, Effective Immediately*, F&W EIM/LIT Alert (7/7/09) (co-author) <www.fenwick.com/docstore/Publications/EIM/EIM_Alert_07-06-09_California_eDiscovery_Signed_Into_Law.pdf>
- *Give P's a Chance*, Recorder (May 11, 2009) ("Policies . . . Protocols . . . [and] Preservation") <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202430718101>> (co-author)
- *Electronic Redaction*, Tech Tip of the Month, State Bar of California LPMT E-News (Mar./Apr. 2009) (content available on request from the author)
- *Information Management for Mergers & Acquisitions – Data Wrangling, Lassoing and Roping at the M&A Corral*, VC Experts Inc.'s *Encyclopedia of Private Equity and Venture Capital* (May 2009) <http://www.fenwick.com/docstore/publications/EIM/VCE_Wrangling_Lassoing_Roping_M&A_Corral.pdf> (co-author), updated version of article previously published in: 12 M&A Lawyer # 9, at 10 (Oct. 2008); and 2008 Bus. L. News No. 2 (Cal. State Bar July 2008)
- *California Guide to Opening and Managing a Law Office*, Ch. 6, Technology, Cal. State Bar (2009), available for purchase at <http://www.calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=10105&id=6249>: *Computer Security, Privacy, and Ethics Concerns*, pp. 268-90 (co-author); *eFiling*, pp. 291-309; *Data backup and management*, pp. 310-28 (co-author); and *Records Retention and Destruction*, pp. 352-67
- *SOX Litigation-Hold Triggers – Public and Private Companies Susceptible to Criminal Prosecution for Obstruction of Justice*, Nat'l L.J. (Mar. 2008) (co-author) <http://www.fenwick.com/docstore/Publications/EIM/SOX_Litigation-Hold_Triggers.pdf>
- *Metadata: To Scrub or Not To Scrub; That is the Ethical Question*, Cal. B.J. (Feb. 2008) <<http://Metadata-MCLE-2-1-08.notlong.com>>
- *Saying Goodbye Just Got More Expensive; Complying With New Ethics Opinion Regarding Returning Electronic Data to Client at End of Representation*, 29 The Bottom Line, No. 2 (Feb. 2008) <http://members.calbar.ca.gov/sections/lpmt/bottomline/pdfs/the-bottom-line_2008_vol-29_no-1.pdf> (Cal. State Bar LPMT Section membership required to use URL; copy available from authors)
- *Secrets Easily Leaked by Friend or Foe In Publicly Filed .PDF Documents*, 13 No. 1 Cyberspace Lawyer 1 (West Jan./Feb. 2008) (co-author) (longer version of *Exposing Redaction* below), available upon request from the authors or by subscription at <http://west.thomson.com/store/product.aspx?r=127062&product_id=37005132>
- *Exposing Redaction*, L.A.D.J. & S.F.D.J. (Oct. 15, 2007) (co-author), available at <http://www.fenwick.com/docstore/Publications/IP/IP_bulletins/IP_Bulletin_Fall_2007.pdf>
- *Privacy Litigation*, chapter 9 of *Data Security and Privacy Law: Combating Cyberthreats* (West 2001 & Supp. 2008) (co-author) <<http://PBCh.notlong.com>> (need Westlaw password to use URL)
- *Redaction Reaction; Do's and Don'ts*, 28 The Bottom Line, No. 3, at 7, 24 (June 2007) <http://members.calbar.ca.gov/sections/lpmt/bottomline/pdfs/the-bottom-line_2007_vol-28_no-3.pdf#page=7> (Cal. State Bar LPMT Section membership required to use URL)
- *Northern California District Court Expands Information Retention Requirements*, F&W Lit. Alert (3/1/07) (co-author) <www.fenwick.com/docstore/Publications/Litigation/Litigation_Alert_03-01-07.pdf>
- *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>
- *E-Discovery Forum*, 8-K Magazine (Cal. Law. Winter 2006) (panelist/co-author) <www.fenwick.com/docstore/Publications/EIM/Winter06_Forum.pdf>

Robert D. Brownstone – eInformation Law & Technology – Bibliography (8/7/09)

Publications (*c't'd*)

- *Web Sites' CDA Immunity: An Ever-Expanding Universe?*, 1 Privacy & Data Protection Legal Rep., No. 11, at 1 (ALM LJN Dec. 2006) (co-author) <www.fenwick.com/docstore/Publications/EIM/Dec06Privacy_website.pdf>
- *Electronic Discovery Focus Of Pending Federal Rule Changes Approved By U.S. Supreme Court*, 15-6 Mealey's Emerg. Toxic Torts 25 (May 2006) (co-author) <<http://FRCP-Lit-ALert-4-06.notlong.com>>
- *The Complexity of Metadata*, EDRM Project (May 2006) <<http://Metadata-EDRM.notlong.com>>
- *USA PATRIOT Act Impasse: E-mail Interception Rules Need Congressional Attention, Too*, 1 Privacy & Data Protection Legal Reporter, No. 2, at 1 (ALM LJN Mar. 2006) (co-author) <<http://wiretap-LJN.notlong.com>>
- *Inefficient Electronic Discovery Management Can Cost Clients* (F&W Litigation Alert 2006) (co-author) <http://www.fenwick.com/docstore/Publications/Litigation/Litigation_Alert_01-04-06.pdf>
- *Collaborative Navigation of the Stormy e-Discovery Seas*, 10 Rich. J.L. & Tech. 53 (2004) <<http://law.richmond.edu/jolt/v10i5/article53.pdf>>
- *How To Sway Litigators To Embrace The Electronic Realm*, 1 Mealey's Litig. Rep. Disc., No. 4, at 38 (2004) <www.lexisnexis.com/applieddiscovery/lawLibrary/newsletter/TheOrangePages_Aug03.pdf>
- *EFiling - The Future is Now*, Findlaw Modern Practice (2003) <<http://practice.findlaw.com/efiling-1203.html>>
- *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>>
- *EFiling: What is it? What are its Implications?*, 19 Santa Clara Computer & High Tech. L.J. 181 (2002) (co-author) <www.fenwick.com/docstore/publications/Litigation/efiling.pdf>
- *Ninth Circuit Clarifies Scope of Fair Use of Computer Code*, F&W Intellectual Property Bulletin (2000) <http://www.fenwick.com/docstore/Publications/IP/IP_bulletins/IP_Bulletin_Spring_2000.pdf#page=8>
- *The National Labor Relations Board at 50: Politicization Creates Crisis*, 52 Brook. L. Rev. 229 (1986) <<http://NLRB50.notlong.com>> (need Westlaw password to use URL)

Featured and/or Quoted in:

- Ryan Davis, *Calif. E-Discovery Rules Welcomed, With Questions*, Tech. Law360 (July 15, 2009), available by subscription at <http://technology.law360.com/print_article/111477>
- Ryan Davis, *Social Networks Could Create E-Discovery Headaches*, Law360 (July 7, 2009), available by subscription at <http://technology.law360.com/print_article/109896>
- John Iasiuolo, *Technology One Byte at a Time: Interview with Robert Brownstone, Expert on Electronic Information*, KDOX 1280 AM, Las Vegas, NV (June 10, 2009) – **podcast/streaming-audio** linked from <<http://www.fenwick.com/pressroom/5.1.1.asp?mid=1088&loc=FN>>
- Mari Frank, *Protect Your Privacy in the Information Age: An Interview With Robert Brownstone, Attorney and Law and Technology Director*, KUCI 88.9 FM, Irvine, CA (May 27, 2009) – **podcast/streaming-audio** linked from <<http://www.fenwick.com/pressroom/5.1.1.asp?mid=1043&loc=FN>>
- Robert Mullins, *Understanding the impact of new state data protection laws*, Compliance & Governance Digest (Feb. 26, 2009) <http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1349287,00.html>
- Correy Stephenson, *Advising clients before they hit 'send'* (Lawyers USA Jan. 2009) <<http://fenwick.com/pressroom/5.1.1.asp?mid=606&loc=FN&p2=23&f=2.23.3&s=1055>>
- Erika Morphy, *The Computer Fraud Act: Bending a Law to Fit a Notorious Case* (E-Commerce Times Dec. 2008) <<http://www.ecommercetimes.com/story/65424.html#>>
- Frank Zeccola, *Landing Thought Leaders in the Press: PR Plays up Legal Expertise to Land in White House Coverage* (BullDog Reporter Daily Dog Dec. 2008) <<http://BullDog-12-8-08.notlong.com>>

Robert D. Brownstone – Information Law & Technology – Bibliography (8/7/09)

Featured and/or Quoted in (*c't'd*):

- Correy Stephenson, *Clients take the reins in e-discovery; Risks, rewards for lawyers* (Lawyers USA Sep. 2008) <www.lawyersusaonline.com/index.cfm/archive/view/id/431854>
- Justin Scheck, *Tech Firms Pitch Tools For Sifting Legal Records* (Wall. St. J. Aug. 2008) <http://online.wsj.com/article_print/SB121936262421062033.html>
- Kathleen Brockel, *Metadata – Ignorance is not bliss* (LSNTAP Aug. 2008) <http://lsntap.org/Blog_Metadata>
- Lawfuel, *Law Firm Fenwick & West Director of Law & Technology, Appointed to NELI Advisory Board* (Aug. 2008) <<http://www.fenwick.com/pressroom/5.1.1.asp?mid=566&loc=PR>>
- Jack Germain, *A Far-Fetched Fix for E-Voting Woes: Open Source* (LinuxTimes Feb. 2008) <<http://www.linuxinsider.com/story/61474.html>>
- Alan Cohen, *Harnessing The Power of EDD; Electronic discovery costs are out of control; Can technology rein them in?*, Law Firm Inc. (Nov. 2007) (copy available upon request)
- Mari Frank, *Privacy Piracy: An Interview With Robert Brownstone*, KUCI 88.9 FM (Jun. 2007) – podcast/streaming-audio at <http://www.kuci.org/privacypiracy/2007Archive.html#06_27_07>
- Allen Bernard, *Data Overload is Overloading the Justice System*, CIO Update (Jun. 2007) <<http://www.cioupdate.com/trends/article.php/3685071>>
- Erika Morphy, *Carving Out New Privacy Rights for E-Mailers*, e-Commerce Times (Jun. 2007) <<http://eCommerce-Times-6-21-07.notlong.com>>
- Anick Jesdanun, *White House e-mail recovery not trivial*, AP (Apr. 2007) <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/13/AR2007041301361_pf.html>
- Pamela A. Maclean, *Oracle E-Discovery Fight Heats Up*, National Law Journal (Apr. 2007) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1176800660744>>
- Alan Cohen, *Data, Data Everywhere: Electronic Data Discovery – How some firms are making big money* Law Firm Inc. (Apr. 2007) <<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1179392701422>>
- Ari Kaplan, *Data Discovery Dep't?*, Law Firm Inc. (Feb. 2007) <www.arikaplan.net/LFI-DataDiscovery.pdf>
- Drew Combs, *Seminar Will Focus on New Issues in Electronic Discovery*, Daily Journal (Feb. 2007) (subscription required to run search at <<http://www.dailyjournal.com/search/index.cfm>>)
- Valerie Helmbreck, *New fed IT rules: What to save and what to dump*, Info. Tech. Adviser™ ([Progressive Business Audioconferences](http://www.fenwick.com/docstore/Publications/EIM/New_fed_IT_Rules_IT_Adviser_1-4-07.pdf) Jan. 2007) <www.fenwick.com/docstore/Publications/EIM/New_fed_IT_Rules_IT_Adviser_1-4-07.pdf>
- Gary Gentile, *Universities vulnerable to ID thieves*, AP (Dec. 2006) <<http://UCLA-Sec-Breach-AP-Article.notlong.com>>
- Paul J. Martinek, *Voicemail, Audio: Subject To e-Discovery*, Compliance Week (Nov. 2006) <<http://Compliance-Week-11-14-06.notlong.com>> (need subscription or free trial to use URL)
- Rob Robinson, *[Gartner] Symposium/ITxpo | E-Discovery*, Info. Governance Engagement Area (Oct. 2006) <<http://infogovernance.blogspot.com/2006/10/symposium-itxpo-e-discovery-what-you.html>>
- Peter Darling, *Seeking Out New Markets: Tapping Into Client Trends for New Business and Bigger Profits*, 32 ABA Law Practice, No. 6, at 28 (Sep. 2006) (cover story) <www.fenwick.com/pressroom/5.1.1.asp?mid=329&f=2.23.3&s=1055&loc=FN&p2=5>
- Marcy Burstiner, *Dumpster Diving: Fenwick & West IT Group on the Cutting Edge*, Law Technology News (Aug. 2005) <<http://www.fenwick.com/pressroom/5.1.1.asp?mid=1377&loc=FN>>
- Ian Hoffman, *Local groups descend on swing states*, Oakland Tribune (Nov. 2004) <http://www.findarticles.com/p/articles/mi_qn4176/is_20041031/ai_n14586853/print>

Robert D. Brownstone – eInformation Law & Technology – Bibliography (8/7/09)

Presentations

- *Compliance*
 - **Gartner: Compliance & Risk Mgmt. Summit** panels 4/09 (Chicago); panel 5/07 (N.O., La); **IT Expo/Symposium** panel 10/06 (Orlando)
 - **MIE Legal Services Corporation (LSC)** national conference – 9/08 (San Antonio)
 - **National Constitution Center (NCC)** national broadcasts – 8/08; 7/08 (Acrobat for Lawyers); 4/07; 3/07; 12/06 <<https://www.constitutionconferences.com/PageData/Group1/Event1480/CCAUDIOConference.pdf#page=4>>
 - **AudioSolutionZ/Eli** national broadcast – 6/08
 - **Workshare** national broadcast (“Data Leakage”) – 5/08
 - **California Society of Health Care Attorneys** (“IT for the Health Care Lawyer”) 4/08 (Napa, CA)
 - **RSA P2P Panel** in SF – 2/07 (“Standard of Care for Outbound Content;” co-facilitator)
 - **Strafford Pubs.** national broadcast (co-presenter) 7/06
 - **Gilbane SF Content Management** Panel 4/06 (SF; co-presenter) <http://lighthouseseminars.com/gilbane_sf_06/presentations/Robert_Brownstone_EDRM-2.pdf>
- *Data & Document Retention/Destruction*
 - **Blue Cross Blue Shield Ass’n Attorneys** – national conference 5/09 (Seattle, WA)
 - **Venture Capital Office Managers Association (VCOMA)** – 4/09 (Stanford, CA)
 - **NCC national broadcasts** – 3/09; 2/09; 1/09; 10/08; 6/08; 3/08; 6/07, 2/07 and 9/06 <<http://www.constitutionconferences.com/98/9W-DL#page=4>>
 - **LegalWorks/Daily-Journal Electronic Discovery After the New Federal Rules** Conference -- 2/07 (Beverly Hills) – Moderator, Retention and Sanctions panels
 - **Progressive Bus. Pubs. (PBP)** national broadcasts – 8/07 <www.pbconferences.com/audio/PageData/Group2/Event1014/AudioConference.pdf#page=3>; 12/06
 - **Strafford Publications** national broadcasts (co-presenter) – 12/06; 10/06 (E-mail Practices); 7/06 (SOX); 4/06
- *eDiscovery/Electronic-Information-Management (EIM)*
 - **Strafford Publications** national broadcasts (co-presenter) – 8/09 (New Cal. Legislation); 2/09 (Data Mapping); 7/08 & 11/07 (Search/Retrieval); 3/06 (Costs); 2/06 (Destruction/Preservation)
 - **State Bar of Cal. webinar** – panelist – New California Legislation – 8/09
 - **Santa Clara U. School of Law** – Adjunct Professor, eDiscovery Law – Summer 2009
 - **Stanford E-Commerce Best Practices Conference** – eDiscovery panelist – 6/09 (Stanford)
 - **Huron/Glasser eDiscovery** (panelist) – 6/09 (San Francisco); and 10/08 (Stanford and San Francisco)
 - **Gartner eDiscovery Workshop** – co-presenter on Search and Risk-Management Panels – 5/09 (Chicago)
 - **NCC nat’l broadcasts** 5/09; 11/08; 4/08, 5/07; and 8/06 <www.constitutionconferences.com/33/9W-DL#page=4>
 - **State Bar of California Emp./Labor Section** 10/08 (San Diego) – “Proactive Information Management Policies and Reactive eDiscovery Strategies”
 - **Litigation Support Today** in DC – 5/08 (“Preservation” co-presenter)

Robert D. Brownstone – eInformation Law & Technology – Bibliography (8/7/09)

Presentations (*c't'd*):

- *EDiscovery/Electronic-Information-Management (EIM) (c't'd)*
 - **Cal. State Bar Section Education Institute** (San Diego, CA) – 1/08 (co-presenter)
 - **American Employment Law Council (AELC)** 10/07 (Ojai, CA) (“Ethical Dilemmas” co-presenter)
 - **National Employment Law Institute (NELI) Advanced Pre-Trial Advocacy Conference** 6/07 (SF + DC); 6/06 (SF + DC); 6/05 (SF + DC); 6/04 (SF + DC); 6/03 (SF); 6/02 (SF + DC; co-presenter) <<http://www.neli.org/programs2.asp?ProgramID=3>>
 - **Nevada State Bar CLE** 5/07 (Las Vegas)
 - **USF School of Law** 3/07 (SF, CA) (Civil Procedure guest lecturer)
 - **NELI Employment Law Briefing** 3/07 (Key West, FL & Las Vegas, NV)
 - **RSA ESAF** in SF – 2/07 (“Legal Discovery” co-presenter)
 - **Bridgeport CE Conference** in SF – 2/06 (Preservation); 2/06 (Tech. Primer; co-presenter)
 - **SCCBA panels** in Santa Clara – 12/05 (“Views from Trenches”) & 5/05 (“Views from Bench”)
 - **IP Inn of Court of Bay Area** debates – 4/04 (Production Forms); 5/03 (Selection Criteria)

- *Electronic Information and/or Privacy in the Workplace*
 - **NCC** national broadcasts, 6/09; 1/08; and 1/07 <<http://www.pbconferences.com/EB/9W-DL#page=3>>
 - **NELI:**
 - **Emp. Law Workshops** 5/09 (SF, CA); 5/08 (Chicago, IL; DC and SF, CA); 5/07 (SF, CA)
 - **Employment Law Briefings** 3/09 (FL and CA); 3/08 (FL and CA); 3/07 (FL and NV)
 - **Emp. Law Conferences** 12/08 (DC & NO, LA); 11/08 (Chicago & SF); 11/07 (NO, LA & SF, CA)
 - **Public Sector & EEO Conference** 8/07 (SF, CA)
 - **State Bar of Cal. Emp./Labor Section** 4/09 panel (Sacramento, CA)
 - **State Bar of Cal. Section Education Institute (SEI)** 1/09 (Berkeley, CA)
 - **Ass’n de Profesionales en Relaciones Laborales** – 10/05 (San Juan, PR)

- *Information Security Obligations - Compliance by Law Firms and Corporate Law Dep’ts*
 - 5/08 (**Witkin Legal Institute** Lecture, Oakland, CA) (co-presenter)
 - 9/07 (**California State Bar**; Anaheim) (co-presenter); 5/07 (**Nevada State Bar**; Las Vegas);
 - 8/06 (**ILTA**; Orlando); 6/06 (**Alameda Bar**); 2/06 (**Bar Association of SF**) (co-presenter)
 - 12/05 (**Fios webcast** <<http://Compl-Fios.notlong.com>>); 8/05 (**ILTA**; Phoenix) (co-presenter)

- *Intellectual Property (IP) as Valuable Business Assets*
 - 12/07 (**San Jose State University**; San Jose, CA) (Industrial Design Program guest lecturer)
 - 11/06 (**California College of the Arts**; SF, CA) (Design Program guest lecturer)

Presentations (*c't'd*):

- *Legal Writing*
 - 1/09; 11/07 **NCC** nat'l broadcasts – **Brief Writing** <www.constitutionconferences.com/6B/9W-DL#page=4>
 - 5/04 **Cisco Systems** worldwide legal all-hands (day-long *Precision Drafting* session)
 - 5/03 **Asian Pacific Bar Association of Silicon Valley** ("*Tips for In-House Counsel*")

- *Metadata Concerns For Litigators, Corporate Attorneys and Non-Lawyers*
 - **Lorman Education Services** nationally broadcast webinars – 8/09; and 2/09

 - **San Diego Cty. Bar Ass'n** webinar – 6/09

 - **Strafford Pubs.** national broadcast co-presenter, 5/09; 10/08; 5/08; 12/07; 9/07; 3/07; 11/06; 3/06; 12/05; 9/05 & 7/05

 - **NCC** national broadcasts/webinars – 3/09; 9/08; 5/08; 2/08; 10/07; 4/07 & 11/06 <<https://www.constitutionconferences.com/PageData/Group1/Event1535/CCAudioConference.pdf#page=4>>

 - **Blue Cross Blue Shield Ass'n Attorneys** – national webinar 6/08; conference 5/08 (Glendale, AZ)

 - **California State Bar** – 9/07 (Anaheim, CA)

 - **SCCBA panel** – 9/07 (*San Jose, CA*)

- *Professional Development – Alternative Careers for Lawyers*
 - Bar Association of San Francisco (6/04)

**APPENDIX F -- Brownstone Materials
Compliance
Partial Bibliography (2/9/09)**

**Comparison (c't'd) —
Big Picture**



ITIL	ISO 27002	COBIT
Provides IT processes	Provides security controls	Provides IT controls + metrics
<i>Security not addressed</i>	<i>Security is the FOCUS</i>	<i>Security not strong suit</i>
Used as delivery mechanism	Used for improving sec. processes/controls	Used as delivery mechanism
HOW	HOW (sec. ONLY)	WHAT

© Kevin Moore, IT Director, Fenwick & West LLP

APPENDIX F -- Brownstone Materials
Compliance
Partial Bibliography (2/9/09)

For Law Firms In Particular



■ TO LEARN MORE:

- R. Brownstone & K. Moore, *Securing Information in Compliance with Ethical Duties, Privacy-Law and Information-Security Best-Practices*
 - ❖ Published as part of the Cal. State Bar's "*Guide to Opening & Managing a Law Office*" (Jan. 2009)
 - ❖ **CHAPTER TEXT AVAILABLE FROM PRESENTER**

APPENDIX G – Brownstone Materials
Computer Technology Terminology
Online Glossaries (2/9/09)

How Stuff Works

<<http://computer.howstuffworks.com/>>

Matisse's Glossary of Internet Terms

<<http://www.matisse.net/files/glossary.html>>

Spyware "Words to Know"

<http://searchsecurity.techtarget.com/tip/1,289483,sid14_qci1089888,00.html>

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/>>

APPENDIX H – Brownstone Materials

DETROIT TEXT-MESSAGING SCANDAL – Additional Articles (@ 8/7/09)

- Tresa Baldas, *Former Detroit mayor skimps on restitution payment, faces possible charges*, Nat'l L. J. (June 4, 2009) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202431222763>>
- Tresa Baldas, *Five lawyers involved in Detroit text message scandal charged with professional misconduct*, Nat'l L. J. (May 20, 2009) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202430873069>>
- Tresa Baldas, *Ex-top aide to Detroit's fallen mayor is out of jail, but won't return to law school any time soon*, Nat'l L. J. (Mar. 17, 2009) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202429113365>>
- Tresa Baldas, *Detroit's ex-mayor sues communications provider for allegedly violating his privacy rights by releasing text messages*, Nat'l L. J. (Mar. 11, 2009) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202428948224>>
- Jim Schaeffer and M.L. Elrick, *Texts show the highs, lows of Kilpatrick's time in office*, Det. Free Press (Mar. 10, 2009) <www.freep.com/article/20090310/NEWS01/903100349/Texts+show+the+highs++lows+of+Kilpatrick+s+time+in+office>
- Tresa Baldas, *Judge orders release of about 1,400 text messages exchanged between Detroit's ex-mayor and former mistress*, Nat'l L. J. (Mar. 10, 2009) <www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202428911242>
- Tresa Baldas, *Prosecutor in Kilpatrick case says he may have violated his plea deal*, Nat'l L.J. (Dec. 3, 2008) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202426436888>>
- Tresa Baldas, *Former Detroit mayor fights to retain law license*, Nat'l L.J. (Dec. 2, 2008) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202426397537>>
- Tresa Baldas, *An attorney looks back at defending Detroit's ex-mayor — and the 'privilege' of standing up for an unpopular client*, Nat'l L.J. (Nov. 5, 2008) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202425783673>>
- Nick Bunkley, *No Plea Deal for Ex-Aide to the Mayor of Detroit*, N.Y. Times (Sep. 16, 2008) <http://www.nytimes.com/2008/09/16/us/16detroit.html?_r=2&sq=kwame%20plea%20deal%20detroit&st=cse&oref=slogin&scp=4&pagewanted=print&oref=slogin>
- Tresa Baldas, *Despite a defense team of 17, Detroit mayor is going to jail*, Nat'l L.J. (Sep. 5, 2008) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202424298419>>
- Tresa Baldas, *Embattled Detroit mayor, local prosecutor locked in a game of 'let's make a deal'*, Nat'l L.J. (Sep. 3, 2008) <<http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202424228869>>
- Tresa Baldas, *Mayor Looks to Ninth Circuit*, Nat'l L.J. (July 24, 2008) <<http://www.law.com/jsp/ca/PubArticleFriendlyCA.jsp?id=1202423214887>>
- Joe Swickard, *Mayor's text defense: It wasn't me; Lawyers: Maybe hacker typed them*, Detroit Free Press (July 9, 2008) <<http://www.freep.com/apps/pbcs.dll/article?AID=/20080709/NEWS01/807090401/1003/NEWS>>
- Monica Davey, *Latest Troubles Put Detroit Mayor's Job at Risk*, N.Y. Times (Feb. 29, 2008) <<http://www.nytimes.com/2008/02/29/us/29detroit.html?pagewanted=print>>
- Jim Schaeffer and M.L. Elrick, *FREE PRESS SPECIAL INVESTIGATION; Mayor Kilpatrick, chief of staff lied under oath, text messages show; Romantic exchanges undercut denials*, Detroit Free Press (Jan. 24, 2008) <<http://Detroit-Mayor-1-24-08.notlong.com>>