

THE INEVITABILITY OF LITIGATION:

New Technologies and Discovery

Blogs, RSS Feeds and Other New Distribution Technologies

By Susan E. Foster

**Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101-3099
(206) 359 8846
<http://www.perkinscoie.com/>**

Susan E. Foster, is a partner in Perkins Coie's Seattle office and is firm wide Chair of the Firm's Antitrust, Consumer Protection and Unfair Competition group. These materials were prepared with the assistance of **Amanda Beane** and **Laura Ewbank**.

TABLE OF CONTENTS

	Page
I. ELECTRONIC DISCOVERY: SUMMARY OF RECENT DEVELOPMENTS.....	1
A. The Zubulake Cases.....	1
B. Federal Rules of Civil Procedure: Key E-Discovery Provisions.....	2
C. Many Companies Have Not Implemented Policies to Address the New Rules or New Technologies	3
D. Potential Sanctions for Failing to Preserve or Produce Electronic Documents.....	4
II. NEW DEVELOPMENTS IN ELECTRONIC COMMUNICATIONS	4
A. Blogs.....	4
B. Instant Messaging	5
C. Joint Contribution Sites: E.g., Wikipedia, YouTube	6
D. Social Networking Sites: MySpace and Facebook.....	6
E. Voicemail and Voice on Internet Protocol (VoIP)	6
F. RSS Feed.....	7
III. THE LEGAL RISKS FOR COMPANIES USING NEW TECHNOLOGIES	7
1. Instant Messaging	7
2. Blogs and Websites.....	7
B. False Advertising and Unfair Competition.....	8
C. Securities Law Violations.....	9
D. Sexual Harassment and Discrimination.....	10
E. Defamation.....	10
IV. DISCOVERY ISSUES ARISING FROM NEW TECHNOLOGIES	11
A. Litigation Holds	11
B. Potential Duty to Preserve Information in Employees' Personal Accounts or Systems.....	11
C. Government Subpoenas of Data and Customer Information.....	12

TABLE OF CONTENTS
(continued)

	Page
V. BEST PRACTICES FOR AVOIDING LITIGATION AND DISCOVERY ISSUES ARISING FROM BUSINESS USE OF NEW TECHNOLOGIES	12
1. Create, Implement and Maintain Clear, Written Corporate Policies.....	12
2. Freeze Automatic Data Destruction Processes When Litigation Is "Reasonably Foreseeable"	15
3. Take Advantage of Safe Harbor Protections Under Digital Millennium Copyright Act ("DMCA").....	15
4. Monitor the Internet for Infringing or Defamatory Use	16
5. Other Helpful Resources.....	16

I. ELECTRONIC DISCOVERY: SUMMARY OF RECENT DEVELOPMENTS

A. The *Zubulake* Cases

- In *Zubulake I*,¹ the court established a three-pronged test for analyzing disputes regarding the scope and cost of discovery of electronic data. First, the court is to determine whether the requested data is readily accessible. Data in an accessible format is discoverable through normal processes and the responding party should pay costs. If the data is stored in an inaccessible format such that the data would arguably be cost-prohibitive to produce, the court must engage in a cost-benefit analysis. As part of this analysis the parties may sample the data to assess its value (e.g. take a small sample of the data from the inaccessible location to determine its relative importance and relevance to the matter at issue). Third, the court will use a seven factor test to determine whether it is appropriate to shift the cost of production to the requesting party.²
- *Zubulake IV*³ stated that parties have a duty to preserve relevant evidence,⁴ including electronically stored data, when litigation becomes "reasonably foreseeable." When litigation is reasonably foreseeable, the company should "suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."⁵ *Zubulake IV* did not require that companies retain backup tapes and other inaccessible data unless they were likely to contain relevant evidence.⁶
- *Zubulake IV* also articulated a three part test for determining when an adverse inference should be held against a party who

¹ *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003).

² *Id.* at 324. The seven factor test used to determine whether the cost to produce should be shifted to the requesting party is: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information. *Id.* at 322

³ *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

⁴ The broad contours of the duty to preserve are relatively clear. That duty should certainly extend to any documents or tangible things (as defined by Rule 34(a)) made by individuals 'likely to have discoverable information that the disclosing party may use to support its claims or defenses.'" *Id.* at 217-218.

⁵ *Id.* at 218.

⁶ *Id.*

accidentally or intentionally destroyed relevant electronic evidence. A jury instruction containing an adverse inference may allow the jury to find that the information was destroyed because it was harmful to the offending party.⁷

- The *Zubulake* case eventually became the basis for recent revisions to the Federal Rules of Civil Procedure that address discovery of "Electronically Stored Information" (ESI).

B. Federal Rules of Civil Procedure: Key E-Discovery Provisions

- ESI is defined separately from "document."⁸
- ESI includes "sound recordings" such as voicemail and VoIP data.⁹
- E-discovery cooperation is mandated and must be addressed in the Rule 26(f) conference.¹⁰
- ESI discovery is limited to production of "reasonably accessible" documents. ESI may be inaccessible due to undue burden or cost. Pursuant to Fed. R. Civ. P. 34(a), the party requesting the documents may ask the court to order production of the documents regardless of cost on a showing of good cause. The cost of production may be shifted to the requesting party if the request is overly burdensome.¹¹ This provision requires a balancing of the

⁷ "A party seeking an adverse inference instruction (or other sanctions) based on the spoliation of evidence must establish the following three elements: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense." *Zubulake IV*, 220 F.R.D. at 219-220.

⁸ Fed. R. Civ. P. 34(a): "Any party may serve on any other party a request (1) to produce...any designated **documents or electronically stored information**..." Also see Fed. R. Civ. P. 26(a)(1): "...a party must, without awaiting a discovery request, provide to the other parties...(B) a copy of, or a description by category and location of, all **documents, electronically stored information**, and tangible things...that the disclosing party may use to support its claims or defenses, unless solely for impeachment."

⁹ Fed. R. Civ. P. 34(a).

¹⁰ Advisory Committee Note to Rule 26(f) (2006 Amendments): "[t]he volume and dynamic nature of electronically stored information may complicate preservation obligations... Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes." See also Rule 26(f)(3)(C): the parties must discuss "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."

¹¹ Fed. R. Civ. P. 26(b)(2)(B). The cost-shifting analysis will likely follow the 7-factor test laid out in *Zubulake IV*. *Supra* n. 2.

burden on the producing party of retrieving the information against the need of the requesting party for the particular data requested.¹²

- A "clawback provision" is included for inadvertently produced privileged documents. Upon notification that a privileged document has been inadvertently produced, the receiving party must promptly return, sequester or destroy the specified document and the subject information cannot be used until the privilege claim is resolved.¹³
- A "safe harbor" provision is included which, absent exceptional circumstances, prevents the court from imposing sanctions on a party for failing to provide ESI lost as a result of the "routine, good-faith operation of an electronic information system."¹⁴
- Sanctions can be imposed on parties who leverage the complexities of e-discovery to impede opposing counsel.¹⁵

C. Many Companies Have Not Implemented Policies to Address the New Rules or New Technologies

- A 2006 survey found that although most companies have policies regarding employees' use of email, very few companies have similar policies for other forms of electronic data, such as blogs and/or instant messaging programs.¹⁶ For example, 1 in 8 firms have fired someone or taken legal action as a result of a blog post, but only 1 in 5 firms have an official policy about blogging.¹⁷
- A recent survey by Fulbright & Jaworski (October 2007) shows that the number of companies allowing and retaining IM is increasing, but that retention times (for IM, voicemail and other technologies) vary significantly between corporations.¹⁸

¹² See Advisory Committee Note to 26(b)(2) (2006 Amendments).

¹³ Fed. R. Civ. P. 26(b)(5)(B).

¹⁴ Fed. R. Civ. P. 37(f).

¹⁵ Fed. R. Civ. P. 26(g)(3).

¹⁶ Bureau of National Affairs, *Survey Finds More Policies Focus on Email Than Blogs, IM*, 179 Lab. & Emp. L. Libr. 522 (2006). See also American Management Association, *2006 Workplace Email, Instant Messaging and Blog Survey: Bosses Battle Risk by Firing Email, IM & Blog Violators* (2006), http://www.amanet.org/press/amanews/2006/blogs_2006.htm.

¹⁷ Bureau of National Affairs, *Survey: Despite Litigation, Firings, Few Firms Possess Blog Policies*, 179 Lab. & Emp. L. Libr. 277 (2006).

¹⁸ Available at <http://www.fulbright.com/index.cfm?fuseaction=correspondence.LitTrends07>.

D. Potential Sanctions for Failing to Preserve or Produce Electronic Documents

- Full or Partial Default Judgment or Dismissal
- Adverse Inference
- Monetary Sanctions
- Attorneys' Fees and costs

II. NEW DEVELOPMENTS IN ELECTRONIC COMMUNICATIONS

A. Blogs

- A **blog** (short for "web log") is a website where entries are written in chronological order and commonly displayed in reverse chronological order. Many blogs provide commentary or news on a particular subject; others function as more personal online diaries.¹⁹ Blogs of particular relevance to e-discovery include:
 - **Corporate blogs:** Many companies, particularly high-technology firms, have made a strategic decision to use blogging as a marketing tool by which to communicate directly with their customers or investors. Examples of this include Intel (<http://blogs.intel.com/>), Microsoft (<http://blogs.msdn.com/>), Google (<http://googleblog.blogspot.com/>) and Sun Microsystems (<http://blogs.sun.com>),
 - **Fan and "gripe" blogs:** Similarly, many firms have fan sites where customers and potential customers may discuss the current and forthcoming products. For example, Apple Computer has www.thinksecret.com and www.macworld.com. Disgruntled consumers or employees may also start blogs that attack a company's products or policies. Examples include <http://www.gapsucks.org/> (regarding clothing store The Gap) and <http://www.mac-sucks.com/> (Apple Computer gripe site).²⁰

¹⁹ See Wikipedia: <http://en.wikipedia.org/wiki/Blog>.

²⁰ Many companies have tried to shut down "___-sucks" sites using a trademark infringement theory; however courts note that most "sucks" sites are not for commercial purposes, but even if they are there is little likelihood of consumer confusion, two essential elements of a trademark infringement claim. See, e.g., *Taubman v. Webfeats*, 319 F.3d 770 (6th Cir. 2003).

- **Personal blogs:** An employee or other individual may facilitate their own personal blog via a personal webpage or social network site. As discussed below, such blogs may become relevant if, for example, an employee begins blogging about her co-workers, company policies or upcoming products or other company information, including competing positions.
- **Satire blogs:** Most recently exemplified by the now famous "Fake Steve Jobs" blog site, there are numerous such sites available on the web. The Fake Steve Jobs blog opines on the general superiority of Apple products from the perspective of its CEO. Fake Steve, who in reality is a journalist from Forbes magazine, was recently ranked 37th on a list of 50 Who Matter Now by Business 2.0 and is frequently quoted by respected media outlets.²¹ Other satire blogs following on Fake Steve Jobs, include: *Fake Steve Ballmer* and *Fake Larry Ellison*
- **Media or Professional Blogs:** Akin to more traditional newspapers many blogs are written by professionals and address a particular topic, such as politics, current events or developments in traditional academic disciplines. See, e.g., <http://www.moresoftmoneyhardlaw.com/> (blog on campaign finance written by Perkins Coie Partner Bob Bauer)

B. Instant Messaging

- Increasingly, companies and individuals are using instant messaging (IM) as a communications device, finding it to be more efficient and effective than email or, with IM/voicemail, typical phone systems. However, IM raises significant concerns for e-discovery: the informal nature of IM conversations makes users less cognizant that these conversations are recorded and discoverable. There are additional risks associated with user identification, authentication, and security. Even if IM is prohibited within the workplace, companies may be surprised to find that their employees have found ways to circumvent the company systems.

²¹ Todd Bishop, *A Moment with Daniel Lyons*, Seattle Post-Intelligencer, October 24, 2007.

C. Joint Contribution Sites: E.g., *Wikipedia*, *YouTube*

- Sites such as *YouTube* and *Wikipedia* allow any user to post, change, add and edit information.²²

D. Social Networking Sites: *MySpace* and *Facebook*

- Social networking sites such as *MySpace*, *FaceBook* and *Friendster* make it easy for individuals to create a personal website that includes text, photos, blogs, and links to other friends.
- Such sites are increasingly used by hiring managers as a means of performing background checks on job candidates.
- Attorneys often use social networking pages as a way to investigate witnesses, claimants, clients and even jurors. (*see, e.g. State v. Goehring*, 2007 WL 3227386 (2007) (reviewing juror's blog reference to trial to determine whether there was juror misconduct); *Gregoire v. City of Oak Harbor*, 2007 WL 3138044 (Wash. App. Div. I) (personal blog used to challenge truthfulness of juror questionnaire). In addition to being used as an informal discovery device, such sites may sometimes be implicated by formal discovery requests.

E. Voicemail and Voice on Internet Protocol (VoIP)

- The new Federal Rules specifically address sound recordings, such as voicemail, as a type of electronically stored information subject to discovery.²³
- VoIP is a means of recording phone messages over Internet cables.²⁴ PC to PC voice mail tools are readily available to individuals as well as businesses.
- Although older voicemail systems did not have the capacity to retain indefinitely all voice mail messages, newer systems have evolved to a point where they can hold a voluminous number of messages and even be converted into data files, allowing

²² Courts have varied with regard to the admissibility of *Wikipedia* entries. *Compare Alfa Corporation v. Oao Alfa Bank*, 2007 U.S. Dist. LEXIS 12771 (S.D.N.Y. Feb. 21, 2007) ("[D]espite reasonable concerns . . . the information provided [in *Wikipedia*] is not so inherently unreliable as to render inadmissible any opinion that reference it.") with *Davage v. City of Eugene*, 2007 U.S. Dist. LEXIS 50337 (D. Ore. July 6, 2007) (unpublished) (*Wikipedia* entry for Balaclava inadmissible).

²³ *See, e.g., Del Campo v. Kennedy*, 2006 WL 2586633 (N.D. Cal. Sept. 8, 2006) (ordering preservation of voice recordings until parties developed a document preservation plan).

²⁴ *Id.*

integration with email. This increased storage capacity has frequently been overlooked by companies in their data retention plans.

F. RSS Feed

- RSS (Really Simple Syndication), which is often called a "feed," "web feed," or "channel," contains either a summary of content from an associated web site or the full text. RSS can also enable the sharing of blog lists (OPML). RSS makes it possible for people to keep up with their favorite web sites, including blogs, in an automated manner that is easier than checking multiple sites manually.²⁵
- RSS feed links are stored on a user's computer system and thus may be subject to discovery. Either the content of the feed or the source of the feed may be determinative in assessing relevancy. Similarly, a subscriber's IP address is normally acquired and stored by companies offering RSS feeds, and this information may be subject to discovery requests.

III. THE LEGAL RISKS FOR COMPANIES USING NEW TECHNOLOGIES

1. Instant Messaging

- Instant messaging is a form of written communication and creates the same legal issues as other written communications whether in hard copy or digital form (e.g., email).
- Retention practices vary considerably for IM, although there are some regulations regarding IM retention. For example, in 1997 the SEC amended its rules to allow broker-dealers to store records electronically.²⁶ Now, the rules mandate that all communication between stockbrokers and their clients—including e-mail and IM messages—be retained for at least three years and remain easily accessible for the first two years.²⁷

2. Blogs and Websites

Posting information to official or unofficial blogs, personal web pages or other websites (e.g., *YouTube*) may create significant legal issues. While many of the issues are the same as those that arise from historical written publications, the internet has

²⁵ See *Wikipedia*, <http://en.wikipedia.org/wiki/Rss>.

²⁶ 17 C.F.R. § 240.

²⁷ SEC Rule 17a-4(b)(4), 17 C.F.R. § 240.17a-4(b)(4); see also Nat'l Ass'n of Sec. Dealers Rule 3110 (2006).

significantly facilitated the proliferation and accessibility of such communications. It is important that companies recognize the potential legal implications that may arise from both formal corporate sponsored postings and blogs, and individual employee posting and blogging activities. For example:

A. Intellectual Property Issues

- Posting of confidential company information may lead to the loss of trade secret status or patentability. And, inappropriate disclosure of confidential information may be a violation of common law duty, confidential agreements, or trade secret laws. Consider in particular technical blogs, fan sites and Wikipedia.
- Posting of third party IP may lead to claims of copyright infringement, trademark infringement, trade secret misappropriation or breach of contract. Consider particularly the risks of postings to technical blogs, *YouTube* and Wikipedia.
- **Example: Apple Computer Litigation.** Apple filed two separate cases against Apple "rumor" websites, alleging that the authors misappropriate Apple's trade secrets by publishing confidential company information. However, these cases took two different angles: in the first, *O'Grady v. Superior Court of Santa Clara County*,²⁸ Apple attempted to identify the source(s) of the leak by subpoenaing a list of contacts from the sites' email providers. In the second, *Apple Computers v. Deplume*, Apple sued the website directly accusing its owner of soliciting information to publish that infringed on Apple's trade secrets.²⁹
- **Example: Best Western Litigation.** *Best Western Int'l v. Furber et al.*, 2007 WL 3274139 (D. Ariz. 2007) (case pending alleging that corporate members disclosed confidential information and defamed company via anonymous blog postings).

B. False Advertising and Unfair Competition

- Providing false or misleading descriptions of a company's products or services may result in violation of consumer protection laws (e.g. Washington Consumer Protection Act (R.C.W. 19.86.020), Federal Trade Commission Act (15 U.S. C.§5)). This risk may arise not only from formal corporate blogs and web pages but from individual postings made by the company's employees and agents,

²⁸ 139 Cal. App. 4th 1423 (Ct. App. 2006).

²⁹ Vauhini Vera, *Apple sues web site run by 19-year-old for revealing secrets*, Wall Street Journal, January 14, 2005.

whether made with full attribution, individually in an ostensible personal capacity or anonymously.

- Providing false or misleading descriptions of a competitor's products or services or engaging in commercial disparagement of a competitor can result in unfair competition, Lanham Act false advertising (15 U.S.C. §45) or similar claims. *See, e.g. Xcentric Ventures LLC. et al. v. Stanley, et al.*, 2007 WL 2177216 (D. Ariz. 2007) (unpublished).
- Although not prosecuted, some companies suffered negative PR when they first entered the blogging world (or "blogosphere") by creating fake blogs (or "flogs") that were heavily veiled advertisements for the companies' products. Mazda was behind a flog purportedly written by a 22 year-old fan that contained links to video clips featuring its new M3.³⁰ Wal-Mart and its PR firm also received criticism for their "Wal-Mart Across America" "flog," where a couple recorded their adventures traveling cross-country while parking their RV at a different Wal-Mart every night. It was later discovered that the couple writing the blog had their entire trip underwritten by Wal-Mart's PR group.³¹

C. Securities Law Violations

- Disclosing material, nonpublic information may result in a violation of securities laws (e.g., failing to include cautionary statements with forward-looking statements,³² or making material misstatements that affect stock prices).
 - **Example: Whole Foods.** Between 1999 and 2006 John Mackey, the CEO of Whole Foods, frequently visited financial discussion boards under a pseudonym, often referring to his own company as though he were merely a stockholder. In addition to comments supporting his own company, he posted negative comments about Wild Oats, a competitor that Whole Foods eventually purchased.

³⁰ Holly Sanders, *Chicken Jerk & Alien Bees, "Viral" Ads Create Buzz but May Not Sell*, New York Post, November 14, 2004; *see also Edelman White Paper Shows How To Brave The Blogosphere*, P.R. News, April 20, 2005.

³¹ The Consumerist, *2006's Biggest Business Debacles*, <http://consumerist.com/consumer/top-10/top-10-biggest-business-debacles-2006-222632.php>.

³² Alys Zeltzer and John Villafranco, *Corporate Blogging: What to Keep in Mind Before You Start Your Own*, 22 *Andrews Telecomm. Industry Rep.* 13 (2007), available at http://www.kelleydrye.com/resource_center/articles_publications/0134/res/id=sa_File1/CMP2414_ZelterComm%20FOR%20WEB.pdf; *see also* Bureau of National Affairs, *Daily Rise in Business Blogging Affects Data Retention, Privacy*, 179 *Lab. & Emp. L. Libr.* 521 (2006).

Harvey Pitt, former chairman of the SEC, told the Wall Street Journal: "It's clear that he is trying to influence people's views and the stock price, and if anything is inaccurate or selectively disclosed he would indeed be violating the law." Pitt added that "at a minimum, it's bizarre and ill-advised" if not per se illegal."³³

- Rahodeb made such comments as: "Would Whole Foods buy OATS? Almost surely not at current prices. What would they gain? Oats' locations are too small," and "while [Wild Oats CEO] Odak was trying to figure out the business and conducting expensive 'research studies' to help him figure things out, Whole Foods was signing and opening large stores in OATS territories." Mackey even went so far as to defend his own haircut when another user poked fun of a photo, stating: "I like Mackey's haircut. I think he looks cute!"

D. Sexual Harassment and Discrimination

- Employees who post inappropriate comments about other employees could face a sexual harassment claim. If posted on an official company website, the company could be subject to suit.³⁴

E. Defamation

- Section 230 of the Communications Decency Act will immunize Internet "publishers" of third-party information, including defamatory remarks, even if that publisher edited the posting or selected it for publication.³⁵ This may include corporations who host email services and websites.
- The Supreme Court recently declined to review a case that would have determined whether or not businesses qualify as third party publishers under the Section 230. However, the lower court held that the company was immune under the CDA as a "provider of interactive computer services" when one employee used its email system to harass another employee.³⁶

³³ See also David Kesmodel and John Wilke, *Whole Foods is hot, Wild Oats a dud—So says "Rahodeb"*, Wall Street Journal, July 12, 2007.

³⁴ Cutler, *Attorneys Say Employers Need to Watch for Pitfalls Employee Blogging Can Create*, *supra*.

³⁵ *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003).

³⁶ *Delfino v. Agilent Techs. Inc.*, 145 Cal. App. 4th 790 (2006).

IV. DISCOVERY ISSUES ARISING FROM NEW TECHNOLOGIES

A. Litigation Holds

- As described in the new Federal Rules, when litigation is "known or reasonably anticipated" a company must stop any automatic deletion of electronically stored information that may be relevant to the case. This may include backup tapes, voicemail recordings or even material not stored by the company, such as private email accounts and blogs.
- While the new Federal Rules have a safe harbor exception for relevant evidence that has been deleted through the routine, good-faith operation of an electronic information system, once litigation is "reasonably anticipated" such automatic deletion procedures must be stopped. The rules provide that the court can still impose sanctions in exceptional circumstances if relevant evidence is deleted.

B. Potential Duty to Preserve Information in Employees' Personal Accounts or Systems

- Employee use of "outside" email accounts or computer systems to conduct official company business presents heightened risks of non-compliance with discovery preservation and production requirements. If a company is aware of this type of use, receives benefit from it and does not take steps to preserve it, the company may be held responsible by the court if that data is destroyed.³⁷
- An employer may have a responsibility to preserve information held in private accounts if a) the employer has a duty to preserve that information, b) the employer has either explicitly or tacitly approved the use of private email for company business, and c) the employer has the ability to exercise influence or control over the private source of information.
- This duty may extend to other forms of private electronic communications and storage devices such as IM, blogs, personal voicemail, PDAs, and cell phones.³⁸

³⁷ See *Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, 2006 WL 2811261 (E.D. Mich. 2006) (holding that defendant company was responsible for spoliation of evidence because it had knowledge of the employee's use of private email account to transmit trade secrets from rival company and failed to take action to stop employee from closing his private email account).

³⁸ *Id.*

C. Government Subpoenas of Data and Customer Information

- By law the federal government can request posted wire or electronic communications, such as blogs or RSS feeds, or subscriber and customer information by obtaining a warrant or through court order or subpoena. The law immunizes service providers from suits arising out of compliance with government requests.³⁹

V. BEST PRACTICES FOR AVOIDING LITIGATION AND DISCOVERY ISSUES ARISING FROM BUSINESS USE OF NEW TECHNOLOGIES

1. Create, Implement and Maintain Clear, Written Corporate Policies

a. Blogging

- For official company blogs, create comprehensive blogging rules and policies that address issues such as appropriate content, language, availability of an official corporate blog for personal use, nondisclosure of trade secret and other confidential information, potential third party copyright infringement, defamation, privacy, disclaimers, compliance with SEC rules and other regulations, data retention, and disciplinary action for employees that violate the policy.⁴⁰
- Implement a separate policy for employees' personal electronic communications, such as blogs, websites and email accounts. Spell out the official company policy on use of home computers and personal communications devices for work related purposes and the appropriate scope of any communications relating to the firm's business.⁴¹ Advise writers of private blogs and websites to post similar disclaimers, identifying opinions expressed as personal and not those of the company.⁴²
- Employers in an at-will state can terminate employees for postings to blogs and other websites that are harmful to the company, harassing to other employees, or that disrupt to the workplace; however, employers should tread carefully in this area. For example:

³⁹ 18 U.S.C. § 2703.

⁴⁰ See, e.g., Sun Microsystems: (<http://www.sun.com/aboutsun/media/blogs/BloggingGuidelines.pdf>), IBM: (<http://www.ibm.com/blogs/zz/en/guidelines.html>), Yahoo!: <http://jeremy.zawodny.com/yahoo/yahoo-blog-guidelines.pdf>.

⁴¹ See Zeltzer and Villafranco, *Corporate Blogging*.

⁴² See Zeltzer and Villafranco, *Corporate Blogging*, *supra*.

- If a company does not enforce its blogging policies uniformly it may risk a potential discrimination claim.⁴³
- Inappropriate restriction and monitoring may result in allegations of:
 - labor law violations e.g. right to organize,⁴⁴
 - whistle-blowing statute violations e.g. if an employee posts a negative opinion of company's product related to safety concerns;
 - First Amendment protection violations—but remember only some apply to private employers. *Cf. Apple Computer, Inc. v. Doe 1*, 74 U.S.P.Q.2d 1191 (2005) (no First Amendment protection for criminal violation (e.g., theft of trade secrets)). One case, *Nickolas v. Fletcher et al.*, 3:06 CV 0043 KKC (E.D. Ky. 2007), is currently pending and challenges state's right to prevent state employees from accessing blogs from state-owned computer systems.
- State law may provide protections for private employee blogs and other lawful activities outside of work.

b. Use of Personal Accounts and Computers

- To avoid the pitfalls suffered by the corporation in *Easton Sports*, adopt a policy that clearly prohibits the use of personal email or IM for company business, or require that private accounts be pre-approved and accessible to employers. Train employees in the policy and implement IT programs to monitor use.
- A recent Washington state case found that employers can access personal email communications if sent through company servers because the employee does not have a reasonable expectation of privacy in those communications after signing a waiver. However, the court declined to extend that right to web-based email accounts

⁴³ *Simonetti v. Delta Air Lines*, No. 1:05-cv-2321 (N.D. Ga. 2005) (suspended pending Delta's bankruptcy case): Delta fired Simonetti, a flight attendant, after she posted a picture of herself in uniform on her blog. She brought a discrimination claim because male flight attendants with similar pictures on their sites were not fired.

⁴⁴ *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) (stating that an employer who improperly accessed an employee's private blog in which the employee posted negative comments about the company may have violated the Railway Labor Act's prohibitions on interference with union organizing activity).

or privileged communications (e.g., husband-wife) sent from company computers.⁴⁵

- Generally restricting employees' ability to save documents offline may help to simplify the discovery process.
- Restricting access to online private email accounts through company servers may also be a helpful step in preventing the theft of trade secrets.

c. Data Retention

- Design a data retention policy that applies to all relevant sources of communications, including official company and unofficial email, voicemail or VoIP, IM, blog posts and websites. Implement and follow a timeline for automatic deletion of electronically stored information.
- Although all forms of electronic information must be addressed in the data retention policy, it does not necessarily follow that all must have the same timeframe for automatic deletion. For example, voicemail messages may be kept for a shorter period than data messages.
- Identify when an employee's personal communications may be included in a litigation hold and educate employees about this policy. Note that this policy must be in place before litigation is anticipated to take advantage of the safe harbor provision in the new Federal Rules.
- Purging ESI frequently, only retaining what is needed as business records or through regulatory requirements, is generally helpful from an IT and business perspective and will help to streamline the e-discovery process.

d. Litigation Holds

- Design a litigation hold strategy that automatically goes into effect when litigation becomes "reasonably foreseeable" under the new Federal Rules.
- Identify what events will trigger a hold, who are key custodians of electronically stored information, what electronic data is potentially relevant (corporate and or personal email accounts, where discoverable evidence is located (servers, portable media,

⁴⁵ *Sims v. Lakeside Sch.*, No. 06-1412 (W.D. Wash Sept. 20, 2007).

external servers, local hard drives, personal computers or PDAs), and the timeframe covered by litigation, taking into particular consideration whether or not archival data, such as backup tapes, will be included.

- Identify who will be the company's 30(b)(6) witness, who can understand and explain the company's IT infrastructure.

2. **Freeze Automatic Data Destruction Processes When Litigation Is "Reasonably Foreseeable"**

- The first step in implementing a litigation hold is guaranteeing that standard data destruction processes for official company data and communications are frozen and that all potentially relevant evidence is preserved. Steps must be taken immediately to make sure that each type of electronic data stored by the company is addressed.
- Appropriate personnel must immediately determine if employees' personal electronic data and communications are part of the hold and take steps to ensure that this data is not accidentally or intentionally destroyed.
- If web based information is destroyed, consider other resources such as the Internet archive (<http://www.archive.org/index.php>).

3. **Take Advantage of Safe Harbor Protections Under Digital Millennium Copyright Act ("DMCA")**

- Companies that allow postings on their websites should take steps to become a "service provider" under the DMCA (17 U.S.C. § 512). The DMCA provides immunity to hosts of websites that inadvertently post protected third party IP if they promptly remove the offending material from their websites after notice. There are three steps required to qualifying:
 1. Designate a DMCA representative with the Library of Congress.
 2. List the company's designated agent on your website. Also post on your website a recap of the DMCA's protocols for removing content.
 3. Design and implement an internal compliance plan based on the DMCA's standard for handling complaints.

Note: The company will not qualify for safe harbor if an employee is the originator of the infringing material.⁴⁶

4. Monitor the Internet for Infringing or Defamatory Use

- Perform Internet searches for the company's name and products so as to prevent or limit damage caused by deliberate or inadvertent references to company products, policies, trade secrets or copyrights.
- Maintain a *Wikipedia* entry about the company in-house, or at least review on a regular basis the entry that others have created. defamation of the company.

5. Other Helpful Resources

Two sections of the ABA are currently working on developing sample policies for companies looking to address the legal implications of new technologies:

- ABA Section of Science & Technology Law, *Blogs and User-Generated Content on the Internet* (2007), <http://www.abanet.org/dch/committee.cfm?com=ST202100&edit=>
- ABA Section of Business Law, Cyberspace Law, *Privacy, Security and Data Management* (2007), <http://www.abanet.org/abanet/common/print/newprintview.cfm?ref=http://www.abanet.org/dch/committee.cfm?com=CL320011>.

⁴⁶ Nancy Flynn, *Blog Rules* (2006).