JTC 650 Public Relations Management
Digital Public Relations 02/2012 **BE SURE TO CHECK FOR POSSIBLE UPDATES**

KEY ISSUES IN LAW AND REGULATION FOR DIGITAL COMMUNICATION MANAGERS

General Principles

- The core of First Amendment's guarantee of free speech lies with *political speech.* Prior restraint can only be employed in rare cases that threaten national security, or involve inflammatory speech directed to (and likely to) incite imminent lawless action, or distribution of obscene material.
- Commercial speech involving the economic interests of the speaker and the audience (such as the promotion of goods and services) is protected to a more limited extent. Regulation of commercial speech is permitted if a) the communication concerns an illegal activity or b) the communication is misleading or deceptive. Also, government regulation on commercial speech is permitted only if a) the government's interest in restricting the speech is substantial and directly advances the government's legitimate interest in protecting citizens, and b) the regulation is narrowly tailored to serve the government's interest. [1]
- Jurisdictions within the U.S. can regulate digital communication as part of responsibilities delegated to the states.
- Jurisdictions around the world exercise the right to regulate online content within their boundaries. As a practical matter, however, nations are limited in their power to control digital communications that originate outside their boundaries.

Privacy laws

- Privacy rights for U.S. citizens are grounded in the Fourth Amendment, which guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[2]
- Federal law prohibits intercepting or recording another's oral or wire communications through the use of electronic or mechanical devices (wiretaps)[3] Note: E-mails sent via an organization's *private* system are not protected.
- In 2000, federal agencies adopted a set of Principles of Fair Information Practices, and Congress has adopted an array of legislation governing the online collection of *personally identifiable information*. Websites are required to adhere to privacy policies designed to protect consumers.

Principles of Fair Information Practices (2000)[4]	
Notice	Collectors must have a policy and disclose practices in understandable language *before* collecting data.
Choice	Consumer must be given options about whether and how their personal data can be used.
Access	Consumers can view and correct the accuracy and completeness of data.
Security	Data collectors must take reasonable steps to assure data accuracy and security.

- Federal law (COPPA) specifically restricts the collection of online data from children under age 13 without obtaining a parent's verifiable consent and grants a safe harbor against prosecution only

[1] Central Hudson Gas & Electric Corp. v. Public Service Commission of New York 447 U.S. 557 (1980)

[2] For details about privacy rights, see Restatement (Second) of Torts § 652A (1965)

[3] Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2510-2522. See also 2701-2710.

[4] Federal Trade Commission, Online Profiling: A Report to Congress, Part 2 (July 2000), p. 3.

if they comply with industry self-regulations equal to or greater than COPPA's requirements.[5]

- Organizations should avoid *negligent enablement of cybercrime* and are increasingly expected to maintain computer security and policies to safeguard against the misuse of legally obtained information by the organization, employees and outsiders. For example, a company's failure to secure financial that results injury to a consumer violate federal law.[6] The majority of U.S. states require companies to inform customers if their personal data been stolen or compromised.
- Personnel need to guard against the unintentional disclosure of personal information, especially in areas such as health care,[7] education,[8] banking and finance,[9] and telephone records.[10] Restrictions apply to the actual *electronic records* as well as the *content.* Laws also require disclosure of the organization's privacy policies and use of personal identifiable information.
- Several states prohibit the remote installation of spyware (malware, ransomware, adware, keyloggers, Trojans, hijackers, dialers, viruses) on a computer without the owner's permission. Several cases have successfully argued that such activity is a *trespass to chattels* or the intentional interference with the possession of personal property that results in injury.[11] Separately, the Federal Trade Commission contends that spyware is a deceptive trade practice. Note: Cookies left on web browsers are not considered spyware.
- Search engines can track a user's website visits, topics research or browser history—activities that are not considered an invasion of privacy. However, the use of that data to *profile* online users is controversial. The FTC continues to monitor the issue of *behavioral tracking* by online advertising networks and has issued a preliminary staff report that asks for public input about a possible regulation that would require a "Do Not Track" setting on personal computer browsers. A notice of proposed rule-making is expected to be issued in 2011.
- California requires companies to disclose their privacy policies on websites and to provide state residents, upon request, an annual report on how information provided in connection with a purchase was shared with others.
- E-mailers are not prohibited from distributing intrusive spam via the Internet, but must allow recipients to opt-out from receiving further messages. Senders must stop sending messages no later than 10 days after a recipient unsubscribes. Opt-out mechanisms must function for at least 30 days after a message is distributed. However, federal law makes it unlawful to send unsolicited commercial e-mail messages to wireless devices, including cell phones, without the consumer's expressed prior authorization. These restrictions do not apply to SMS (text) messages.[12]

Copyright

- Creative works of various types (text, images, videos) can be protected from exploitation by others as an *intellectual property* right. A U.S. copyright is good for the life of an individual copyright holder plus 70 years (or 95 years for a work created for hire).[13]
- Organizations should guard against the *direct infringement* by avoiding the use of copyrighted content without obtaining proper permission. The most blatant example involves *pagejacking,* where an offender copies content and puts it on a site that appears to be the real site, and then invites users to the fake site through deceptive means.
- Operators of websites and Internet service providers (ISPs) are protected against prosecution for copyright violations involving *user-generated content*. Under the "notice-and-takedown" rules within the *safe harbor provision* of U.S. copyright law*,* site operators or ISPs must investigate and remove challenged materials, if appropriate, upon receipt of written notice.[14] Otherwise, operators can be sued for *contributory infringement.*

[5] Children's Online Privacy Protection Act (COPPA), 1999. 16 CFR § 312.
[6] Gramm-Leach-Billey Act
[7] Health Insurance Portability and Accountability Act (HIPPA), 1996. 42 USC 1320d-6.
[8] Family Educational Rights and Privacy Act (FERPA), 1974. 34 CFR 99.
[9] Gramm-Leach-Billey Act 15 USC 6801-6809. See also SEC Regulation S-P.
[10] Telephone Records and Privacy Protection Act, 2007.
[11] Sotelo v. DirectRevenue LLC 384- F Supp. 2d, 1219 (ND, Ill. 2005).
[12] Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, 2004.
[13] Copyright Act. 17 U.S.C. 302 1051-1129.
[14] Digital Millennium Copyright Act (DMCA), 1998 amended the Copyright Act of 1976. 17 USC 101-See esp. Sec. 512. DCMA also implements in the United States several international copyright treaties.

- Owners of copyrighted digital materials can incorporate digital rights management (DRM) within their works to prohibit unlawful duplication. DRM tools cannot be lawfully disabled by others.[15]
- Merely linking to a copyrighted website or web page is permissible as long as the document is not duplicated. This includes *deep linking* to pages or elements within another website. However, *inline linking* to a photo or other element on another website and then displaying it on a website may constitute the creation of a *derivative work* and can result in claims of contributory infringement. Such practices might be prohibited under a website's term of use but are difficult to enforce unless the website requires visitors to affirmatively assent to comply.[16]
- Similarly, website operators cannot "pass off" another website as their own and should avoid using *frames* to simultaneously display parts of others' websites and thus give the impression that the displayed content is original.
- Webcasters must acquire *performance rights* to copyrighted sound recordings in the same way as over-the-air radio stations.
- "Fair use" guidelines allow for citation or inclusion of limited excerpts of copyrighted materials when used for instructional purposes, as part of a review or critique, or as part of a public commentary on an important issue.
- File-sharing and piracy (theft and resale) of entertainment fare intended for sale are illegal.[17] Organizations should discourage such activity.
- Organizations that want to encourage republication of materials can still limit how materials are used can do by registering content through the private program operated by Creative Commons (www.creativecommons.org)
- Computer software or applications created for promotional purposes can be copyrighted or, alternatively, patented as computer software that is a novel, non-obvious, useful business process. If offering a promotional application, a good policy is to develop a "click-through" licensing agreement where users agree to the terms of use prior to downloading the software. In most cases, software and apps are licensed or leased for use (not sold), and creator retains ownership rights

[15] 17 USC 1201-1205.

[16] Ticketmaster v. Tickets.com 54 USPQ 2nd (BNA) 1344.

[17] MGM Studios v. Grokster 545 U.S. 913 (2005)

Trademarks/Service Marks and Trade Names

- Trademarks are a form of intellectual property similar to copyright. Federal trademark registrations are administered by the U.S. Patent and Trademark Office[18] while state trademark registration is dealt with by each state's trademark office. Trademark owners enjoy the right to an injunction against a person who uses the mark in commerce in a manner that is likely to cause consumer confusion ("trademark infringement). Also, owners of famous and distinctive trademark enjoy the right to an injunction against a person who uses the mark in commerce in a manner that is likely to cause dilution by blurring or tarnishing ("trademark dilution"). This principle has been applied in an array cases involving strikingly similar web domain names.[19]
- Avoid using the trademarks or service marks of another organization in a way that mistakenly suggests that one organization is affiliated, approved, or sponsored by the other. However, the nominative use of another's trade name in is permitted for descriptive purposes – as long as use of the term is reasonably necessary and does not suggest sponsorship or endorsement.
- Website designs are a form of *trade dress* that can be protected under the trademark laws. Copying or mimicking a design is a form of unfair competition if the effect is to create a false designation of origin or misrepresentation likely to cause confusion, mistake or deception as to the origin or sponsorship.[20]
- Under the U.S. anti-cybersquatter law, trademark owners can recover ownership damages from others who act in "bad faith" to register website domain addresses that are identical to or confusingly similar to an existing distinctive trademark. Bad faith means the intent was to capitalize financially or to harm the goodwill enjoyed by the trademark owner. This generally involves purposely diverting traffic away from

[18] Trademark Act of 1946 (aka Lanham Act) and Trademark Dilution Revision Act 2006. 15 USC 1125.

[19] Visa International Service Association v. JSl Corp. 533 F. Supp 2nd 1090 (D. Nev. 2007); Mattel Inc. v. Internet Dimensions, Inc. 55 USPQ 2nd 1620 (S.D. N.Y. 2000); Hasbro Inc. v. Internet Entertainment Group, Ltd. 1996 WL 84858 (W.D. Wash, 1996); Toys "R" Us v. Akkaoui 40 USPQ 2nd 1836 (N.D. Cal. 1996)

[20] Peri Hall & Assoc. v. Elliot Institute, 2006 WL 742912 (W.D., Mo, 2006)

the trademark owner's own site(s) when users search for terms on a search engine.[21]

- Organizations can seek damages from *typosquatters* who register domain names that are misspelled variations of popular sites merely for the purposes of exploiting the errors and diverting traffic.[22]
- Trade names can be within the domain names of gripe or complaint sites operated by critics as long as the trademark is not used for commercial purposes.[23] Similarly, trademarks and trade names can be used in *parodies* and critical commentaries as part of the exercise of political free speech.[24]
- Trade names can be in use text or primarily for informational purposes. In fact, the FTC encourages the use of *comparative advertising* that fairly compares features of multiple brands within the same ad. Note: Many trademark owners also vigorously pursue the misuse of trade names as generic terms in order to prevent losing the distinctive value of their trade name. (Example: Do not use Kleenex® to refer to all *facial tissues.*)
- Advertisers can use trademarked brands name of competitors in search ads (a practice known as *piggybacking*).[25] Search engines can also recommend as *keywords* as part of offering their service. However, at least one case ordered a defendant to include the plaintiff's name as a "negative keyword" to avoid confusion.[26] Banner ads can include trade names for search engine results as long as the name of the advertiser is clearly identified in order to avoid possible confusion.[27]
- Importantly, organizations should be cautious in incorporating trade names of competitors in metatags on web pages (used to identify page content) if the effect is to divert traffic from a legitimate trademark owner's site.[28] However, such use can be considered fair use as long as the purpose was not to divert traffic.[29] Utah's state supreme court similarly ruled that pop-up ads scheduled to appear over a competitor's website did not constitute unfair competition or interference with commerce.[30]

Right of *Publicity*

- Individuals retain the right to sell their image or words in conjunction with the endorsement of commercial products or the advocacy of positions on political or social issues. Thus, digital communicators should not *appropriate* an individual's image or words without permission.[31]
- Merely reporting about a person's presence or participation in a *public* event is not a violation of the person's rights of privacy or publicity. Similarly, using statistics of real-life baseball players in an online fantasy baseball league was not found to be misappropriation.[32]
- Similar to copyright law, website operators have been exempted from tort action involving *user-generated content* that might violate another's right of publicity.[33] Unlike copyright law, however, site operators are not liable in tort actions for failing to remove challenged content.
- Photographers working for websites or online news organizations might be subject to regulations in certain states pertaining to *paparazzi*—photographers who aggressively stalk and photograph public figures for profit.

Deception and Promotional Practices

- Commercial speech that is false or knowingly deceptive is not accorded First Amendment protection and is subject to prosecution for deception by regulatory agencies under federal and state laws.

---

[21] Anticybersquatting Consumer Protection Act (ACPA), 1999

[22] Vulcan Golf LLC v. Google Inc. 552 F Supp.2d 752 (N.D. Ill. 2008)

[23] Lamparello V. Falwell 420 F.3d 309 (4th Cir. 2005).

[24] Louis Vuitton Malletier SA v. Haute Diggity Dog, 507 F.3d 352 (4th Cir., 2007)

[25] Rescuecom Corp. v. Google, Inc., 456 F. Supp. 2d 393 (N.D. N.Y. 2006)

[26] Orion Bancorp., Inc. v. Orion Residential Fin. LLC 2008 WL 816794 (M.D. Fla. 2008)

[27] Playboy Enterprises v. Netscape Communications Corp. 354 F.3d 1020, (9th Cir., 2004)

[28] North Am. Med. Corp. v. Axiom Worldwide Inc. 522 F.3d 1211 (11th Cir., 2008). Brookfield Communications, Inc. v. West Coast Entertainment Corp. 174 F.3d 1036 (9th Cir. 1036. Niton Corporation v. Radiation Monitoring Devices, Inc.27 F. Supp. 2d 102 (D. Mass., 1998)

[29] Playboy Enterprises Inc. v. Welles 279 F.3d 796 (9th Cir. 2002)

[30] Overstock v. Smartbargains, Inc. 192 P.3d 858 (Utah, 2008)

[31] Restatement (Third) of Unfair Competition §46 (2005); Restatement (Second) of Torts 652A (1965).

[32] CBC Distribution and Mktg. Inc. v. Major League Baseball Advanced Media LP 505 F.3rd 818(8th Cir. 2007)

[33] Carafano v. Metrosplash.com. Inc., 339 F3rd 1119, 1112 (9th Cir., 2003); Communication Decency Act of 1996 (47 USC § 230(c).

- All digital communications are considered "advertising" by the Federal Trade Commission for purposes of regulating unfair trade practices and deceptive advertising.[34]
- The FTC requires full disclosure of material connections, if any, between endorsers and the seller of an advertised product that might affect the weight or credibility of the endorsement. This rule outlaws *blogola* (paying for paid posts) but also covers comments by consumers in videos, blogs, and postings on message boards as well as endorsements appearing in traditional media or in person-to-person situations.[35]
- The FTC has obtained injunctions and taken actions against deceptive practices involving the redirection of web traffic. These include *mousetrapping* techniques designed to make it difficult to exit a site, obstructive practices where access to a desired site is repeatedly blocked, and prompts that result in asking users to download unknown or undesired software.
- All digital communications by related to pharmaceuticals are considered *labeling* by the U.S. Food and Drug Administration and require whatever *contraindications* (instructions and precautions) specified for particular drugs. Drug companies have virtually abandoned the use of search-based text advertising following FDA complaints about inadequate disclosures. .
- Federal Communications Commission rules prohibit the display of web addresses during children's programming on TV if the website is selling a product. The FCC permits displaying website addresses in other situations only if specific criteria are met.[36] During any program, broadcasters may not display the address of a website that uses characters from the program to sell products or services.
- E-mailers are prohibited by federal law from sending *unsolicited commercial e-mail* (UCE) containing misleading information or using deceptive subject headers. E-mailers must include a functional return address in all correspondence. [37]
- The European Union adopted an Unfair Commercial Practices Direction in2005 that prohibits advertising that distorts economic behavior—including misleading actions and omissions and aggressive advertiser practices.[38]

Financial Disclosures

- The Securities and Exchange Commission and major stock exchanges have embraced the online distribution of financial information to investors—including the distribution of annual meeting notices, proxies and annual reports and encourages online disclosures on websites.[39]
- Publicly traded companies (firms that issue stocks, bonds, etc.) must avoid the unintentional disclosure of *material* information, both online and offline. Materials facts are those that might influence an investor to buy or sell. Publicly traded companies must disclosure material information *promptly* and *fully* to the widest possible audience whenever any material information is disclosed. The purpose is to avoid problems with insider trading.[40]
- *Pump and dump schemes* by issuers of securities, brokers or speculators involve sending bullish mass e-mails or promoting a security in chatrooms or forums, running up the price and then selling shares for a profit. Such practices are illegal under both federal and state laws.
- Special rules apply to what publicly held companies can during the *quiet period* during which a registration statement for a security is pending at the SEC prior to be declared effective and for 90 days after issuance.
- Internet road shows and webcasts must comply with all SEC regulations.[41]
- Brokerage firms, banks and other financial organizations are required to archive websites, e-mails and social media messages (blogs, Twitter, SNS, etc.) to assure compliance with securities regulations.

Objectionable Material

- The U.S. Supreme Court has ruled that indecent material and pornography cannot be banned on the Internet.[42] However, states can regulate obscenity in keeping with the three-prong test outlined by the Supreme Court.[43] The display or

[34] Federal Trade Commission Act 15 USC 45
[35] 16 CFR 255, especially Sec. 255.5
[36] 47 CFR 73.670; 47 CR 76.225
[37] Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, 2004. 15 USC § 7701-7713.
[38] Directive 2005/29/EC.
[39] SEC Internet Availability of Proxy Materials, RIN 3235-AJ47 (March 30, 2007).
[40] U.S. Securities and Exchange Commission Regulation FD.
[41] SEC Release No. 33-8591—Securities Offering Reform.
[42] Ashcroft v. ACLU 535 US 564 (2002)
[43] Miller v. California 413 US 15 (1973).

possession of pornography featuring children is specifically prohibited to discourage the exploitation of children.[44] Similarly, public libraries and schools are required by law to install filtering software to prevent access to adult material by children. [45]

Defamation

- Organizations and others can attack others through attack sites, complaint/gripe sites and parody sites as well as disparaging comments on forums and chats, blogs or social networking sites, but should avoid *defamation.*
- Parties attacked online can sue an identifiable detractor for defamation or *libel* under (civil) tort law for damage to their reputation. To be libelous, a statement must actually be published, identify the *plaintiff, and* be false and harmful. A private person merely needs to demonstrate *negligence in* a majority of states whereas a *public official* or a *public figure* must show *actual malice*.[46] Three basic defenses against a libel case involve *truth*, *fair report privilege* (the statement was originally made *in court* on the floor of a legislative body *and merely repo*rted) *and fair comment* (a stat*ement of opin*ion versus fact).
- Similar to the U.S. laws applicable to traditional news media, website operators and providers of interactive computer services (including social networking sites) cannot be sued for libel merely based on defamatory comments posted by third-party users. However, they can be liable if they were paid to post the content, contributed materially to its creation, reason to know of the defamatory content or promised the author and then failed to remove it.[47]
- *Hate speech* (inflaming public opinion against certain groups) is permitted, but online speech inciting *imminent violence* is not protected.[48]

Other Organizational Issues:

- **Illegal and Fraudulent Activities**. Activities that are prohibited in the offline environment are prohibited online. E-commerce websites operate under the same rules as other commercial entities under the Uniform Commercial Code adopted by all 50 states. The FTC also has the authority to prevent fraudulent, deceptive and unfair business practices. These include social engineering or manipulation of user and identity theft. *Phishing* involves sending deceptive e-mails that refer recipients to a landing page that asks for financial or other personal data.
- **Electronic Records and Signatures.** Certain procedures are streamlined in Uniform Electronic Transactions Act adopted by all states except Illinois, New York and Washington (which have their own laws). The Electronic Signatures in Global and National Commerce Act (E-Sign) validated the use of electronic signatures on contracts but guaranteed consumers the right to obtain agreements in written form.
- **Product Liability.** Courts make no distinction between learning about potentially dangerous products online or offline. Similarly, the use of digital communications (such as video games) is not considered a product for which a claimant might sue for injury, damages to property, personal injury, wrongful death or economic loss.[49]
- **System Integrity.** Website operators generally have the right to bar abusive practices specified in their Terms of Use (including excessive spam, access by search engine bots and installation of spyware). Operators may sue as a tort involving *trespass to chattels* but might be required to demonstrate substantial damages.[50] Federal laws provide various criminal and civil protections to prevent outsiders "without authorized access" from wiretapping wire or telephone communications[51] and from accessing a wire or electronic communication in electronic storage.[52] This includes theft of trade secrets and sensitive economic information by foreign states.[53]
- **Trade Secrets** Theft of trade secrets might be prosecutable under the one of several federal

[44] PROTECT Act of 2003. 18 USC 2252-2260.
[45] Children's Internet Protection Act (1999). US v. American Library Assn, 539 US 194 (2003)
[46] New York Times v. Sullivan 376 U.S. 254 (1964); Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967)
[47] Communications Decency Act of 1996, Sec. 230. (Title V of the Telecommunications Act of 1996] Barrett v. Rosenthal 146 P.3d 510,526 (Cal. 2006); Perfect 10 Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007).
[48] Brandenburg v. Ohio, 395 U.S. 444 (1969). Planned Parenthood of the Columbia/Willamette, Inc. v. Am Coalition of Life Activists 289 F.3d 1058 (9th Cir. 2002)
[49] James v. Meow Media Inc. 300 F3d 683, 688 (6th Cir. 2002).
[50] CompuServe, Inc. v. Cyber Promotions, Inc. 962 F Supp. 1015 (S.D. Ohio 1997); EBay Inc. v. Bidders Edge, Inc., 100 F. Supp. 2d 1068, 1067 (N.D. Cal. 2000); Intel Corp. v. Hamidi, 71P 3d 296 (Cal. 2003)
[51] Computer Fraud and Abuse Act 18 USC 1030.
[52] Stored Communications Act 18 USC 2701-2710.
[53] Economic Espionage Act 18 USC 1831-1832

laws pertaining to illegal access of electronic communications. Disclosing trade secrets to the public (including distribution e-mail or a web site) can prosecute under state laws if the content is divulged to the public for the first time.[54]

- **Employee Use of E-Mail Systems.** Private employers can monitor and regulate the use of private e-mail systems by employees without restrictions. Public employers have a variety of legitimate reasons for doing so. These include business and client confidentiality, legal and securities compliance, and avoiding of misrepresentation of false claims. Private firms also must protect trade secrets and system, and prevent employees from engaging in discriminatory, harassing or threatening activities. For public employees, an intrusion upon an employee's *reasonable expectation of privacy* has been weighed against the employer's legitimate purpose.[55]
- **Employee Activities Outside of Work**. Except in the case of communications related to organizing by labor unions, employees of private employers (who are *at-will* workers) can be fired for posting (negative) comments or any other work-related information on blogs, social networking sites, chats, forums and wikis. Government workers and contractors similarly can be dismissed, demoted or reprimanded.
- **Labor Communications.** Federal law forbids employers from interfering with, restraining, or coercing employees in the exercise of rights relating to organizing, forming, joining or assisting a labor organization for collective bargaining purposes, or engaging in protected concerted activities, or refraining from these activities.[56] This includes allowing reasonable e-mail communications. In early 2011, the National Labor Relations Board settled a case involving an employer that illegally fired an employee who criticized her supervisor on her Facebook page.
- **Notices of Employee Rights.** Employers are required to post the contents of the NLBR's Notification of Employee Rights poster on any intranet or internet site where personnel rules and policies are customarily posted.
- **Equal Opportunity.** Digital communications are subject to the same requirements and guidelines applicable to traditional communications requiring the affirmative promotion of equal opportunity in the areas of finance, employment and housing. Requirements include inclusion of required equal opportunity insignias and statements and the avoidance of discriminatory language and graphics. Anti-discrimination laws also apply to data collection practices used by online services that use the data to classify users based on sex, ethnicity, etc.[57]
- **Foreign Agents Registration**: Organizations and individuals that are compensated to represent foreign nations or corporations are required to register with the Department of Justice.[58]
- **Access for Disabled.** Although websites have not been deemed to be placed of public accommodation under the Americans with Disabilities Act of 1990, website operators have been challenged to provide access for impaired users. Federal law (known as Sec. 508) requires that disabled individuals seeking information or services from a federal have access to, and use of information and data comparable to that provided to nondisabled individuals.[59]
- **Electronic Notifications and Signatures.** Organizations might be subject specific regulations pertaining to the acceptability and electronic messages and electronic signatures.
- **Subpoenas Related to User-Generated Content**. Under federal anti-terrorism laws, the FBI can subpoena customer records, such as telephone records of suspected terrorists. Presumably this includes digital records about postings on organization-sponsored blogs, chats, social networking and media sharing sites.[60]
- **State Sales Taxes --** Organizations are required to collect applicable state sales taxes on any transaction involving buyers within any state in which the seller has a physical presence (such as executive or branch offices or a warehouse).
- **Records Retention.** Digital records must be maintained in accordance with applicable federal and state laws and regulations. Digital files are also subject to federal and state freedom of information acts- governing public records.

[54] Uniform Trade Secrets Act adopted by 46 states. Or the Restatement (Second) of Torts (D.C. Massachusetts, New York, Texas).

[55] O'Connor v. Ortega, 480 US709 (1987)/

[56] National Labor Relations Act

[57] Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir., 2008)

[58] Foreign Agents Registration Act (1938)

[59] Workforce Investment Act of 1998. 29 U.S.C. § 794d. .

[60] USA-Patriot Act 2001 18 USC 2516, 18 USC 2503, 2509.