

# CCH<sup>®</sup> GUIDE TO COMPUTER LAW

Guide to Computer Law—Number 293

## Practitioner's Perspective by Holly K. Towle, J.D.



**Holly K. Towle** is a partner with Kirpatrick & Lockhart Preston Gates Ellis LLP (K&L Gates), an international law firm, and chair of the firm's E-merging Commerce group. Holly is located in the firm's Seattle office and is the coauthor of *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons). Holly.Towle@KLGates.com, 206-623-7580.

## Top 10 Common Mistakes Made on Websites

With spring on the way, company websites make good candidates for a spring-cleaning list. To that end, here are ten top mistakes often made on websites:

1. Missing You
2. Bad Timing
3. Inauthentic Authentication
4. Inappropriate Imitation
5. Muddled Amendments
6. Escaped Notices
7. Programming Puzzlement
8. Footer Failure
9. Contractual Blindness
10. Insecure Privacy & Security

These mistakes tend to result from paying too little legal attention to site programming or terms of use. Fortunately, all can be remedied.

**1. Missing You.** The good news about websites is that they attempt to use language that is accessible to users; the bad news is that this can create new problems. Consider sites with this kind of language:

- By using this site you agree to be bound by all terms and conditions.
- You agree to indemnify and hold us harmless....
- You agree not to upload viruses or access unauthorized areas....

Who is you – the person reading the screen (user), someone else, or both?

In a consumer site, "you" is the consumer because there is no one else (although in a community property state, "you" might be the user individually and/or the user's marital community, a difference that can be material). In a business-to-business site (such as a manufacturer's site for distributors, or a charitable organization's site for independent companies dispersing aid), "you" might be: (1) the user as an individual, *i.e.*, even if the user is an employee of the distributor or the aid company, the user's liability is personal; (2) the user acting solely as an agent for his or her principal, *i.e.*, an employee acting only as agent for the distributor or aid company, thus binding that entity as opposed to the employee; (3) *both* the user individually and the user's principal; or (4) the user individually, but only when he or she is a sole proprietor, *i.e.*, the user "is" the distributor or the aid "company" (there being no distinguishable, legal entity).

**Practitioner's Perspective** appears periodically in the monthly Report Letter of the CCH Guide to Computer Law. Various practitioners provide in-depth analyses of significant issues and trends.

A common mistake is to fail to explain which “you” is intended. Given the variety of possible answers, this can create ambiguity and consequent litigation.

But there is no blanket answer. If the promise is that “You agree not to upload viruses or access unauthorized areas,” it may well be that an employee should be individually liable: the threat of individual liability may be the most effective means of discouraging that conduct and such conduct may be outside the user’s scope of employment. On the other hand, if the promise is that “You agree to indemnify and hold us harmless against all breaches of the Terms of Use,” one employee typically is not individually liable for breaches by another, and only the employer will usually have the financial means to make good on the indemnity. In short, the answer to who “you” is may vary per site and per provision.

**2. Inauthentic Authentication.** Establishing the “you” is advisable but not the same as knowing who the human user *actually* is or the user’s level of authority to act for a principal. To impose liability on the person a site intends to be liable, there must be a way to “attribute” the conduct or contract made by the user to the person who is supposed to be bound. If a user orders a stereo online using Joe’s account, but Joe says he never ordered anything, can the site attribute the order to Joe? If Joe actually does place a large order for Acme Inc., but Acme says the order was beyond Joe’s contracting authority, can the site attribute the order to Acme?

It is critical to develop an attribution procedure and/or to obtain an agreement allowing “attribution” of contracts or conduct to the person intended to be bound. There is no one-size-fits-all solution and attribution procedures are typically tailored to the risks involved. For example, in high risk transactions, recent guidance for federally insured financial institutions says they may not use “single factor” authentication (such as only a password) but should use multifactor authentication. For anyone looking for an overview of alternative authentication methods, the guidance may be of interest. See Federal Financial Institutions Examination Council, “Authentication in an Internet Banking Environment” (2005), FIL-103-2005.

**3. Bad Timing.** Many sites contract with users regarding the terms for use of the site. But the contract may be ineffective if it comes too late. For example, if damage can occur *before* a contract consenting to venue, requiring arbitration, or limiting damages is formed, the desired contract clause can be irrelevant to the pre-contract harm. See *e.g.*, *Williams v. America Online, Inc.*, 7 ILR (P&F) 3019 (2001) and *Lopez v. Charles Schwab & Co.*, 118 Cal.App.4th 1224, 13 Cal.Rptr.3d 544 (2004) The lesson is to get the contract in place before anything covered by the contract can occur.

**4. Inappropriate Imitation.** It often appears that some sites simply copy terms from others. This can work when the two sites are doing exactly the same thing and making the same

business decisions, but usually that is not the case. Sites do different things, which means different laws and risks need to be treated with corresponding terms. For example, what good will a disclaimer of warranties copied from a site selling goods do for a site offering services? Disclaimer laws governing the sales of goods are not the same as those governing services. What good will it do a site providing stock brokerage services to copy terms from a site providing information about how to knit a child’s bedspread? The former, but not the latter, should deal with liability for inaccurate information, and only the former carries a significant risk of consequential damages (*e.g.*, from a trade based on inaccurate information). Failure to tailor terms of use to actual activities, risks and governing law can be a mistake.

**5. Muddled Amendments.** In an ongoing contractual relationship, one or both parties will often need to amend a contract. E-commerce does not change contract modification laws. The mistake made by some sites is to fail to deal with those laws or to make assumptions about which laws apply.

For example, where there is no ongoing relationship, such as when site users have no continuing right to visit a site, there is no legal requirement that terms of use on Monday need to be the same as the terms of use for Tuesday—the site owner sets the rules for each visit just as a store owner may set its rules (“no shoes, no service”). Notice of material changes can be appropriate, but consent to amendments is not required. But when there is a contractual right to visit the site, such as where a user pays a fee for a two-year access contract, then there is an ongoing contract and amendments need to be made in ways that satisfy contract law. Mixing up the two scenarios can lead to problems, just as can failing to comply with applicable contract law.<sup>1</sup>

**6. Escaped Notices.** There are several new federal laws pertaining to various aspects of online life, some of which provide safe harbors or other protections if the online service provider provides certain notices. Yet many sites do not provide these notices even though they could prove beneficial.

For example, under the Digital Millennium Copyright Act, an online service provider generally can avoid liability for infringing material placed on its servers by others, if it complies with the statute. Part of compliance is to register for, and then provide a notice of, the site’s copyright agent, the point person for receiving notices from copyright owners that the site contains infringing material. Another part of compliance is to provide notice of an adopted termination policy for repeat infringers. The Communications Decency Act provides immunity for an interactive computer service against obscene, defamatory, or other objectionable material placed on the site by users (*e.g.*, in a chat room), but contains a notice requirement regarding the commercial availability of filtering software for limiting access by minors. The CAN-SPAM Act requires notice from Internet access services in order to make unlawful harvesting or dictionary attacks

against site email records.<sup>2</sup> Sites can forego the protection of these statutes, but the question is whether they know they are doing so.

**7. Programming Puzzlement.** A modern puzzle is why some sites programmers continue to appear unaware of electronic commerce rules providing consequences for noncompliant programming? For example, the Uniform Electronic Transactions Act, a statute adopted by numerous states, allows an individual to avoid a contract unless the site provides reasonable error correction procedures.<sup>3</sup> Although many sites do so, the procedures are not necessarily obvious to the user. Similarly, the federal Electronic Signatures in Global and National Commerce Act has extensive provisions regarding the ability to provide electronically a consumer notice that is required by law to be provided on paper, yet some sites seem to be unaware of those rules.<sup>4</sup> The same act requires electronic records to meet certain rules and the consequence of not meeting them can be contract invalidity where the law otherwise requires the record to be in writing.<sup>5</sup> The mistake here is to ignore the new rules.

**8. Footer Failure.** Sites containing links to “Terms of Use” in their footers are ubiquitous. Many operators think that as long as there is a link to the terms somewhere in the footer, then anyone using the site is bound by those terms. That is not a safe assumption. Case law suggests that, without more, bare references or references not seen may be inadequate to form the contract. See *e.g.*, *Specht v. Netscape Communications Corp.*, 306 F3d 17 (2nd Cir. 2002).

**9. Contractual Blindness.** The *Specht* case illustrates another common mistake, *i.e.*, an assumption that contract law is somehow magically satisfied or suspended online. The *Specht* court finds no magic: if you want a contract you still need to make one under normal contract laws. Those laws do not adapt automatically to the Internet, however, so new thinking is required. The Uniform Computer Information Transactions Act<sup>6</sup> and its Official Comments provide examples of how to deal with adaptation and are easier to find and review than case law; UCITA is also predictive of case law so makes a good foundation for compliance. However one gets there, compliance is necessary.

As an example, consider a requirement that a disclosure be “delivered.” In the offline world, the disclosing party might hand over the disclosure and require the recipient to sign a receipt; or it might mail the disclosure and keep a record of the mailing. What about online? Some sites assume that simply having a link to the disclosure is sufficient—would the same assumption be made if offline, the disclosing party kept a pile of disclosures on a table and put a notice at the door stating that the table was in X room of the building? The disclosures

certainly would be *available*, but would they be *delivered*? Delivery can occur online, however, such as by forcing the user to click on the link to the disclosure. Just as in the offline world the user may decide not to read the disclosure or may even throw it away—but it will have been delivered if the link is made “non-bypassable.”<sup>7</sup> If the relevant rule requires delivery in a form the consumer may *keep*, then the delivered copy should also be downloadable and/or printable. If a consumer is involved and the law requires the disclosure to be delivered on paper, online delivery will likely need to comply with some of the new e-programming rules (see No. 7).

**10. Insecure Data Protection & Security.** Data protection and information security is not the same as it used to be: America is now in the forefront of aggressive regulatory interpretation and enforcement in these areas, notwithstanding its early reputation as a being behind the curve. Between a proliferation of state adoptions of “security breach notification” statutes,<sup>8</sup> “spyware,”<sup>9</sup> identify theft<sup>10</sup> and similar statutes, and Federal Trade Commission enforcement actions regarding privacy policies and information security,<sup>11</sup> the U.S. is now ahead of the curve. Yet many website privacy and information security policies have not been, but should be, changed to deal with the current enforcement environment.

Spring cleaning allows easier breathing. Outdated websites may be good candidates for any company’s spring cleaning list.

## Endnotes

- <sup>1</sup> For more discussion of this topic see Chapter 8 of Raymond T. Nimmer and Holly K. Towle, *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons).
- <sup>2</sup> See *id.* for more details.
- <sup>3</sup> *Id.* at Chapter 6.16.
- <sup>4</sup> *Id.* at Chapter 11.09.
- <sup>5</sup> *Id.* at Chapter 4.15[3](Supp.).
- <sup>6</sup> See Chapter 5 of Raymond T. Nimmer and Holly K. Towle, *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons).
- <sup>7</sup> See *e.g.*, Federal Reserve Board Staff Commentary to 12 CFR § 205.17(b) at No. 3.
- <sup>8</sup> See Chapter 12 of Raymond T. Nimmer and Holly K. Towle, *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons).
- <sup>9</sup> *Id.* at Chapter 2.29.
- <sup>10</sup> *Id.* at Chapter 15.
- <sup>11</sup> See *e.g.*, *In the Matter of DSW Inc.*, File No. 052 3096 (Dec. 2005) and *BJ’s Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 2005)(FTC enforcement actions for inadequate information security practices in circumstances where the actual inadequate practices were not statutory or the subject of previous regulatory elucidation).