

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

Guide to Computer Law—Number 286

## 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.

## Employment Law—Taking a Fresh Look in the E-Information Age

Employment law doesn't look the same anymore and this column lists a few of the reasons. Employers may wish to take a fresh look in light of new laws regarding information or doing business electronically. Some act as an "overlay" to employment law, creating a combination with surprising results. Savvy employers may wish to consider taking advantage of opportunities presented by, or qualifying for defenses under, some of the new laws. They should also train (or re-train) employees. Here are a few examples in question-and-answer format.

**Employee Internal Policies.** *Is there any reason to review employment policies in light of the new laws?*

Yes. There are many new factors, not all of which are obvious. For example, in the United States there are new federal laws providing various protections to online service providers such as AOL, Yahoo, MSN, and the like. By meeting conditions, the ISP can obtain certain immunities or defenses. For example, if a user of an AOL chat room defames someone, the user is liable for defamation but AOL is not, if it has taken certain steps and avoided others.

Under some of these laws, the definitions are broad enough to encompass employers providing e-mail or online access, and that creates a new world for employers. In the example, the employer may still be liable for defamation if the employee acted within the scope of employment or the employer was too involved with aspects of the communication, but the liability of the employer should no longer be assessed solely under traditional defamation law relating to employees and employers.

Of course, policies also remain important for traditional reasons—but updating may be in order. For example, computer fraud and abuse acts make it a crime to access most computer systems without authority, but many employees have authority to use their employer's network so the laws will not be relevant to that use. However, these laws also tend to include a concept of *exceeding* authorized authority, so policies or the like should deal with that concept. And what about employee blogs? Those are not simple outlets to blow off steam—they can involve significant legal issues and have unexpected impacts. For example, assume an employer carefully crafts public statements about a particular topic in order to avoid being viewed later as a "public figure" when the company or its officers claim that they have been "defamed." If they are not "public figures," defamation is easier to prove. But will the employer or its officers be assigned "public figure" status if an employee blogger has been publicly wrestling online regarding

**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.

all aspects of the debate? The existence of the blog and the facts surrounding it will complicate the litigation and may, depending upon the facts and documentation, influence the outcome.

**Spam.** *Employees in Division X are keen to send e-mails about a new promotion to all customers. Employees in Divisions Y and Z are not happy because they send promotional e-mails too, and they don't like Division X contacting "their" customers. Are there legal issues there?*

Yes, given anti-spam laws. Under U.S. federal law, for example, Division X cannot send its e-mail to a customer who already told Division Y that the customer did not want to receive further e-mails from the employer. There are ways to control the scope of that opt-out, but coordinating and tracking what promotional e-mails go out to whom is legally required. There are even new rules regarding text messages to mobile phones. Employee policies should be updated to deal with these kinds of issues. See *e.g., Feland Limited Partnership v. Digi-Tel Communications, LLC*.<sup>1</sup>

**Metadata.** *Employees used to write notes on hard copies of documents being negotiated—now they do the same thing electronically by black-lining and using comment tools etc. Does that make a difference?*

Yes, and employees should be trained to understand the differences. A hard copy covered with messy notes and revealing strategy and internal conversations seldom leaves the premises—only a nice clean copy goes out with all of the back-and-forth omitted. But if the nice clean copy is electronic, those notes are likely “metadata” that might still be there. Essentially, metadata is hidden data generated during creation and editing that can reveal persons who worked on the document, the name of the organization in which it was created or worked on, information concerning prior versions, recent revisions, and comments or redlining inserted in the back-and-forth between employees, including attorney-client communications. Ethical rules for attorneys are beginning to require removal of metadata and even beginning to forbid the other side from reading it when sent inadvertently—but those rules do not apply to non-attorney-client exchanges. “Metadata” should be included as part of the new training employees receive in our e-economy.

**E-mail Communications.** *Is it true that a recent U.S. case said e-mails can't be used for notices to employees?*

No. The lower court in *Campbell v. General Dynamics Government Systems Corp.*<sup>2</sup> certainly made it sound that way, but the First Circuit made a course correction. Actually, the notice in question was ineffective, but not because e-mail was used. It was ineffective because it did not meet standards for notice required by federal arbitration law (at least in this court's rather extreme view of contract law). The First Circuit explained:

We...acknowledge that the district court's opinion does exhibit a high degree of skepticism about the use of e-mail in this context. We do not share that skepticism: we easily can envision circumstances in which a straightforward e-mail, explicitly delineating an arbitration agreement, would be appropriate...

In all events, the Electronic Signatures in Global and National Commerce Act (E-Sign Act)... likely precludes any flat rule that a contract to arbitrate is unenforceable under the ADA solely because its promulgator chose to use e-mail as the medium to effectuate the agreement. ...By its plain terms, the E-Sign Act prohibits any interpretation of the FAA's “written provision” requirement that would preclude giving legal effect to an agreement solely on the basis that it was in electronic form.

E-Sign generally creates an equivalency for the validity of paper and electronic records in myriad transactions.<sup>3</sup> That new fact of life has numerous ramifications for employers. Read on.

**E-Contracting.** *Employees are trained that only the purchasing department may make purchase contracts and that oral contracts don't count (at least in some industries). Do E-Sign and similar state laws impact that training?*

Absolutely. The new rule of thumb is this: e-mails are “writings.” Not only can they meet “writing” requirements (such as a contract calling for amendments only in “writing”), but they can also be “signed writings.” That means an e-mail can form a contract, even one that must meet a statute of frauds. Agency law has not changed and it is still necessary for an employee to have real or apparent authority. But in settings where an employee is empowered to deal with an issue and does so by using an e-mail leaving a record that is very different from an oral telephone conversation where each party later disputes what was, or was not, said. E-mails are records and will be discovered and examined to see if they contain the elements necessary to make, waive, or amend a contract—they will also be used to interpret the contract when parol evidence is admissible. And employers should not assume they can address this reality with a “no oral agreements or amendments” understanding. Those aren't much use in many settings.<sup>4</sup>

The good news (depending upon who you are) is that e-mails and online systems can be used to resolve the age-old problem of the “battle of forms.” That is where one business sends a purchase order and the other sends an invoice, and each thinks they have a contract on “their” terms when, in fact, they may have a contract but not on the terms each thinks. Electronic systems allow one party more easily to require the other to agree to their terms before proceeding. Of course, not all businesses are willing to take on that confrontation—

but even those who choose not to will be faced with systems created by businesses making the opposite choice. Unless employees are trained to recognize a contract when they see one, contracts can be formed or altered, like it or not.

### **Obtaining, Using, or Transferring Personal Information.**

*What kinds of new rules are there?*

There are lots of new, non-uniform laws impacting various activities of employers who use or hold computer information. For example, several U.S. states have new laws restricting the electronic transfer of certain data, such as social security numbers or other kinds of data that an employer would have on an employee, unless the data is encrypted. That kind of law obviously impacts e-mails sent from one office to another, for example. There are laws beginning to restrict the use of genetic data such as New Mexico's Genetic Information Privacy Act which literally makes it unlawful for a person to use genetic information in employment. The federal government just passed the Private Security Officer Employment Authorization Act which, generally speaking, regulates obtaining and using background checks on employees performing certain security services (*e.g.*, the night guard), including rules regarding employee consent and access to background check information. This is in addition to the employer's traditional duties under the Fair Credit Reporting Act and new duties under amendments made to that act by the Fair and Accurate Transactions Act (regarding identity theft).<sup>5</sup> And of course, there are privacy and data protection laws, both domestic and foreign, that increasingly impact employers or some of the information they hold, transfer and use (whether regarding employees or customers).

### **Information Security.** *Do any of the new information security laws impact employers?*

Yes. It is difficult to find a business that is not impacted, directly or indirectly, by new information security statutes. Some of the statutes only cover "consumers" but others cover "individuals," and most businesses have "personal information" or "personally identifying information" on individuals, whether they be employees or customers. This "personal" information isn't necessarily private in the traditional sense, *i.e.*, a name and birth date are *protected* under some data protection statutes, even though they are not commonly viewed as *private* (*e.g.*, The Wall Street Journal recently *published* the name and birth date of the proposed nominee for the U.S. Supreme Court, and some people routinely supply name and birth date to enter a contest for a free tote bag). The new statutes exist at both the state and federal level<sup>6</sup> and coverage and content varies with the statute. The statutes variously create rules regarding security of information and its disclosure and disposal,

including disposal or transfer of devices containing the information (*e.g.*, donating a computer to a school).

Even if an employer can chart a course through these statutes that does not trigger a need to comply, it may be subject to *contracts* requiring security. Examples would be contracts with a merchant bank to turn in customer credit card "slips," or contracts with other businesses to which the employer is a service provider. Some of the statutes require a covered entity to require its service providers to provide a similar level of security, so the statutory requirements will eventually "trickle down" domestically and internationally via contract, *i.e.*, from covered entities to "non-covered" entities.

And, of course, there is always the common law. It is developing in ways that will need to be watched. In *Bell v. Michigan Council 25 AFSCME*,<sup>7</sup> for example, \$275,000 was awarded against a union for negligently allowing an employee to take home personal data on union members in order to work from home. The employee's daughter was convicted of identity theft involving several union members and the court found the "special relationship" necessary to create a duty sounding in negligence on the part of the union:

As plaintiffs' representative union, defendant has an obligation to act on behalf of, and in the best interests of, plaintiffs....It follows that part and parcel of that relationship is a responsibility to safeguard its members' private information. And society has a right to expect that personal information divulged in confidence, especially to an organization such as a union whose existence is for the benefit of the union members, will be guarded with the utmost care. Moreover, from a control standpoint, defendant is in the best position to protect plaintiffs because it controls who has access to its membership lists.

Notably, the union had no procedures or safeguards in place to ensure confidentiality and the court viewed the general risk of identity theft as foreseeable, even though the conduct of a particular criminal is not. Other courts treat the underlying doctrines very differently so it is likely best to do as this court suggested and confine its unpublished holding to its unique facts. The case illustrates, however, the push and pull that may be placed on common law concepts in years to come.

And then there is the U.S. Federal Trade Commission. Its enforcement actions in recent years regarding privacy and information security have been predicated on the failure of businesses to live up to the text of their privacy policies (which typically include security provisions). The FTC has consistently grounded its enforcement actions in literal disconnects between the policy text and actual practice,

claiming that the disconnect is an unfair practice. *In a dramatic shift away from that foundation*, in 2005 the FTC filed suit against BJ's Wholesale Club, Inc., claiming that BJ's "failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice."<sup>8</sup>

Is that really true as a legal matter? The action was not premised on an alleged violation of any privacy or security statute or common law duty, so the question should turn on case law under concepts of unfair acts and practices. No judicial answer will be available, however, because BJ's entered into a consent order.

The new laws regarding doing business electronically or information have many more impacts on employers than can be discussed here, including international impacts. For example, businesses in other countries can be impacted because they do business with U.S. companies or because they have U.S. affiliates. In short, knowing employment law is no longer enough, just as knowing e-commercial law is not enough – there are new overlays.

#### ENDNOTES

- <sup>1</sup> *Felland Limited Partnership v. Digi-Tel Communications, LLC*, 864 A.2d 1027 (MD 2005)(creation and dissemination by cell phone company's employee of facsimile ad violating federal rule against unsolicited faxes went beyond scope of employment where facsimile advertising was prohibited by company).
- <sup>2</sup> *Campbell v. General Dynamics Government Systems Corp.*, 407 F.3d 546, 556-557 (1st Cir. 2005).
- <sup>3</sup> See Holly Towle and Raymond Nimmer, *The Law of Electronic Commercial Transactions* at Chapter 4 (A.S. Pratt & Sons 2003-2005)(explanation of E-Sign and similar state laws such as the Uniform Electronic Transactions Act) (hereafter "*E-Commercial Law*").
- <sup>4</sup> See e.g., *Lamle v. Mattel, Inc.*, 2005 WL 27554 (Fed.Cir. CA 2005) and *E-Commercial Law* at Chapter 13.08.
- <sup>5</sup> For an explanation of identity theft and FACTA, see *E-Commercial Law* at Chapter 15.
- <sup>6</sup> For a discussion of the range or details of some of these new laws, see *E-Commercial Law* at Chapter 12.07[2](disposal of data), Chapter 12.14 (social security numbers), and 12.17 (security).
- <sup>7</sup> *Bell v. Michigan Council 25 AFSCME*, 2005 WL 356306 (MI Ct. App., 2005) (unpublished).
- <sup>8</sup> See FTC documents at <http://www.ftc.gov/opa/2005/06/bjswholesale.htm>.