

## 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.

**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.

## E-Commerce for Everyone

Everyone with a computer or similar device—cellular telephone, “crackberry,” home computer, laptop, computer at work, or geo-positioning device for a boat or car—they’re all participating in e-commerce. They don’t think of it that way because many confine the concept to websites engaging in online sales. But in reality, e-commerce is e-business and even e-“life,” and everyone is living it.

This column takes a look at a few of the impacts that computer information, technology and new e-commerce laws are having and their transformative effect.

**1. The E-Overlay.** E-commerce is nowhere and everywhere at the same time. It is so pervasive that it is not possible to confine it to any one legal area. It is more like a transparency sheet for an overhead projector. Lay all of the new laws impacting e-commerce on top of any business transaction today and you will see a transaction that is different from one for which the overlay is ignored. The overlay shows numerous new substantive rules, causes of action, and defenses.

An example is Section 230 of the federal Communications Decency Act. This section provides powerful immunity to providers of “interactive computer services” but many companies have never heard of it. Under § 230, AOL or MSN do not have liability for much of what customers say or do in their chat rooms because that content is provided by “another” information content provider (the customer or other visitor) instead of by AOL or MSN. But the definition of “interactive service provider” is broad enough to include other website operators even if they are not access providers like AOL; it’s also broad enough to include an “ordinary” business such as an employer operating a company system. This was recently recognized in *Delfino v. Agilent Technologies, Inc.*<sup>1</sup>, where the CDA was applied to a corporate employer because it was a provider of interactive computer services—even though those services pertained to employees instead of Internet users.

What is of interest here is not that the CDA immunity extends to such employers—that is inherent in the definition. What is noteworthy is that the CDA, an act new for the information age, is available for use by such employers but most do not think about in connection with internal systems.

**2. Data Protection.** Many of the new laws concern privacy and data protection. These laws and their emphasis are not widely understood by businesses for a very good reason: some of them contradict previous laws and legitimate business practices.

*State v. Farmer*<sup>2</sup> is a 1996 example of the traditional view of commercial data, *i.e.*, that there is no legitimate expectation of privacy in information a person reveals to a third party such as evidence of a transaction with a business. The case involved a warrantless collection by an insurance company of sales receipts from a merchant—the insurance company suspected that the consumer had altered the receipt submitted and wanted to compare the merchant’s version to the consumer seeking reimbursement for property loss. The consumer claimed the receipts were “private” and thus could not be seized without a warrant; the court held that the seizure did not violate the Washington constitution. That result reflects traditional U.S. law, *i.e.*, some information is truly private and may not be shared with others absent the data subject’s consent, but most commercial information is not private and may be shared for a variety of purposes. Indeed, without the ability to share information, fraud and identity theft cannot be prevented.

Fast forward and compare *Farmer* with a 2007 New Jersey case, *State of New Jersey v. Reid*.<sup>3</sup> In this case of first impression a New Jersey superior court determined that the New Jersey constitution affords significantly greater rights than the Fourth Amendment to the U.S. Constitution and that New Jersey is alone in finding an implied right of informational privacy “no matter how trivial, that can be traced or linked to an identifiable individual.”<sup>4</sup> In New Jersey, the information that prevented the fraud in *Farmer* will not be shared—it will be too expensive to invoke legal process to obtain the information and what reasonable cause will sustain a warrant request: such information might be obtained merely as a matter of commercially reasonable practices and due diligence relating to fraud prevention, as opposed to particularized suspicions that might be necessary to obtain a warrant. More senior New Jersey courts may reverse the ruling, but it still illustrates the trend in data protection which is to assume that “data protection” is a paramount good with no competing public policies. This is an assumption that will lead to the very harms sought to be avoided (*e.g.*, fraud and identity theft, but it will take some time to strike an appropriate policy balance.

**3. Information Security.** Securing personally identifying information has become a necessity in e-business. This is so for at least two reasons: (a) increasingly laws require security for personally identifying data; and (b) laws regarding security breaches punish the business victim.

**(a) More laws require information security for personally identifying information.** When data security laws first began to appear, they were sector specific so many companies were not covered. That is an increasingly rare because covered entities are required to contract with their service providers for similar levels of security. Also, some states are going beyond sector-specific coverage to impose generally applicable security obligations.

There are also new statutes requiring notice of data security breaches, each differently defining the “personal information” which must be the subject of the breach. This makes it difficult and costly to create practical and compliant systems and procedures. The Federal Trade Commission is the poster child in this regard. It is creating its data security rules on the fly, *i.e.*, through enforcement actions it is utilizing different definitions,<sup>5</sup> and even different lists of what constitutes “unreasonable” security. To regulate data security, the FTC is using its general power to regulate against “unfair acts or deceptive practices” under Section 5(a) of the Federal Trade Commission Act,<sup>6</sup> and making an inaccurate statement in a privacy policy, or failing to employ “reasonable and appropriate security measures to protect personal information,” can violate the act. Whether the FTC is correct as a legal matter, and whether it has the authority to take that position without legislative action, remains to be seen. In the meantime, the FTC is making and enforcing data privacy and security laws even though no statute or regulation provides a guiding course.

**(b) Laws regarding security breaches punish one of the victims.** In a typical security breach, an individual steals a purse, briefcase or laptop, or exceeds their authorized access to data stored on an employer’s computers, or hacks into website data. Identity theft is not a crime generated by corporations or legitimate businesses—it starts with wrongdoing by an individual. Although laws exist to punish that individual if he or she can be caught, an article in the Wall Street Journal indicates that those laws are seldom enforced or, even when enforced, put the individual back out on the street.<sup>7</sup> According to the article, this lack of effective enforcement makes identity theft an increasingly popular crime for a widening variety of small time (and big time) criminals.

Who is the victim of the crime? There are two. The first is the person whose identity is stolen, *i.e.*, the data subject, and current laws focus on protecting that individual. But there is a second victim, *i.e.*, the business or other person holding the data that is stolen. When the identity thief steals a laptop, or when an employee sells data to an identity theft ring, the business holding that data is also the victim of a crime and will suffer significant losses. What is startling about legislation allocating all of this loss to the business is the legislation’s failure to recognize that the business too is a victim and that the legislation often risks creating inappropriate and disproportionate results.

An example is the result in *Kehoe v. Fidelity Federal Bank & Trust*,<sup>8</sup> where the court decided that the Driver’s Privacy Protection Act (“DPPA”) does not require proof of actual damages in order to award \$2,500 in statutory damages. Fidelity paid one penny per driver’s name to Florida which, unbeknownst to Fidelity, had not complied with the new DPPA allowing drivers to opt out of sales of their data. Fidelity paid \$5,656 for 565,600 names to which it mailed

solicitations for refinancing auto loans. An award of statutory damages of \$1.4 billion (\$2,500 per violation) was entered against Fidelity. In denying certiorari, two Supreme Court justices expressed concern about this “enormous potential liability” but, because the case had been remanded, agreed with denying certiorari. They commented that “it may later be appropriate for us to consider granting certiorari.”<sup>9</sup> One would hope so.

This example illustrates several points beyond disproportionality and focus other than on the actual wrongdoer: it also shows how businesses can be taken by surprise by modern data protection laws. Names and address are in every public telephone book and are in many public records (*e.g.*, real estate and tax records); and names and addresses of drivers were routinely sold by states for many years. Yet Fidelity incurred a liability of \$1.4 billion for buying those very names. As Dorothy would say to Toto, “we are not in Kansas anymore.”

**4. Mergers and Acquisitions.** The impact and number of new “e” law also impact the value of a business. This impact should be taken into account, for example, in due diligence done before acquiring a company or its assets. Ordinary due diligence, such as in mergers and acquisitions, needs to take the new “e” rules into account. The focus of this new area is on issues arising from doing business electronically. Simply increasing the scope of a due diligence is not a solution, however. The new laws governing business done electronically (in whole or part), and the information age itself, require: (i) taking another look at some of the fundamental premises of typical merger and acquisition agreements and revising them to deal with new subject matters; and (ii) altering due diligence procedures to incorporate new concerns.

For example, assume an acquirer is valuing a target in part for its customer list at X amount per customer; acquirer intends to use the list to send marketing materials touting the enhanced services available from the merged entity. But *having* customers is not the same, any more, as being permitted to send marketing e-mails to them. In an increasing number of settings, customers may “opt-out” of receiving materials by e-mail and companies possessing lists are obligated (by law or their privacy policies) to track those customers who do for a number of years to ensure that they do not receive further emails.<sup>10</sup> If the due diligence process ignores this issue, the acquiring party may pay for something it is not really getting (and, perhaps, allocate too much value for tax, accounting and other purposes to the list).

**5. E-Contracting by Employees.** Employees in U.S. industries are routinely trained that only the purchasing department may make purchase contracts and that oral contracts don’t count (at least in some industries). But if the new “e” laws are applied to those practices, a different result emerges. Under new laws enabling electronic contracting, the new rule of thumb is this: e-mails are “writings” and they can also be

“signed writing.” That means an e-mail can form a contract or make an amendment requiring a “signed writings”—this comes as a surprise to many, even though it should not be surprising by this date.

The good news (depending upon who you are) is that emails 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 take it on will be faced with systems created by businesses making the opposite choice. In any event, a broader group of employees may be forming or altering contracts by email or on websites, absent sufficient training.

**6. Intellectual Property as Ubiquitous.** The U.S., at least, is no longer an industrial economy where the main source of wealth is the manufacture and sale of goods and physical commodities. Information drives the U.S. economy and wealth is generated from the creation, distribution, servicing and use of websites, of software (in and outside of the workplace), of information, data and of other intangible information. Information, however, is fundamentally different than goods. If one breaches a contract for the sale of goods, contract law tends to be the primarily relevant law. If one breaches a license for intellectual property, the background law is very different: federal patent and copyright law stand behind much information and the consequence of breach can include infringement. Although intellectual property laws have long existed, indeed, they have constitutional roots, they have not been the stuff of commerce except in recent years. In short, there is a new learning curve.

**7. E-Discovery in Litigation.** A sure sign that e-commerce has come of age is issuance of a set of rules expressly dealing with how e-data will be produced and handled in litigation. In the U.S., litigation tends to be a national sport and there are a new set of rules. On December 1, 2006, amendments to the Federal Rules of Civil Procedure (“FRCP”) addressing “electronically stored information” took effect.<sup>11</sup> These rules amount to a codification of practices that have been evolving and employed in the federal courts under the pre-existing discovery rules. The amended rules address these aspects of electronic data in the discovery process: definition of electronically stored information; early discussion of its treatment in the discovery process; format of production; accessibility of electronic information; a “safe harbor” for routine electronic information systems management; and inadvertent production of privileged material. Each requires businesses to rethink how, why and for how long they keep electronic information.

**8. Payment Cards.** A sea change is taking place regarding merchant rights and obligations regarding payment cards such as credit cards and debit cards. At least the following three aspects of the new “e” laws impact every retailer accepting a payment card.

**A. Receipts.** A federal law<sup>12</sup> now requires what many state laws also require, *i.e.*, truncating credit and debit card numbers on electronically printed receipts provided at the point of sale. No more than the last 5 digits may appear and the expiration date also may not appear. The law became effective on December 4, 2004 as to cash registers or other devices that electronically print receipts and were first put into use *on or after* January 1, 2005. For machines that were in use *prior to* that date, the law became effective on December 4, 2006. Yet examination of a receipt from merchants even today will show that some merchants still are not aware of this law.

**B. PCI.** A new payment card industry standard, “PCI,” was adopted by the major credit card associations and companies in 2005 to promote uniform security for payment card transactions. The current standard is “Payment Card Industry Data Security Standard (DSS) v 1.1” which replaced as of December 31, 2006, “DSS v. January 2005.” This standard is not easy or inexpensive to comply with and many merchants are struggling to get into compliance. Noncompliance is literally subject to heavy fines. The extent to which they will be enforceable raises contract law issues that can be complex.

**C. Processing Agreements.** Statutes regarding data security and notice of data security breaches, have created a need to take another look at payment card processing contracts. Typically, these have imposed security obligations on merchants that previously assumed that the processors would have secure systems. That is not necessarily so today, as illustrated by an FTC enforcement action against a data processor, *In the Matter of CardSystems Solutions, Inc., and Solidus Networks, Inc., Doing Business as Pay by Touch Solutions*, File No. 052 3148 (Feb. 2006). Also, perfect security is not possible, so even adequate systems will fail for various reasons. This means that notice of a security

breach may need to be given by the merchant, so the merchant’s contract with the processor should deal with that scenario when possible.

The above is only a glimpse of new laws impacting doing business electronically or operating in an information age. We are only beginning to realize the consequences, legal and otherwise. Taking a closer look is advisable and often imperative.

### Endnotes

- 1 *Delfino v. Agilent Technologies, Inc.*, 145 Cal.App.4th 790 (2006) (13 CCH Computer Cases ¶49,239).
- 2 *State v. Farmer*, 80 Wash. App. 795, 911 P2d 1030 (1996).
- 3 *New Jersey v. Reid*, 2007 WL 135685 (NJ Super. Ct., 2007) (13 CCH Computer Cases ¶49,259).
- 4 *Id.* at 4.
- 5 See *e.g.*, *In the Matter of Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens*; File No. 052 31(2006)(defining “personal information” in a settlement agreement significantly more broadly than the statute at issue and more broadly than a statute concerning the same subject matter (data disposal) but under which no charge was made).
- 6 15 USC 45(a).
- 7 See Andrea Coombes, “Identity Thieves Steal to Buy Groceries – Easy and Low Risk: A Perfect Crime for Everyday Life,” *The Wall Street Journal* (2/15/07).
- 8 *Kehoe v. Fidelity Federal Bank & Trust*, 421 F3d 1209 (2005), *pet for cert. den.* 2006 SL 173456 (US 2006).
- 9 *Id.* 2006 SL 173456 at 1.
- 10 See *e.g.*, E-Commercial Law at Chapter 13.07[4] (spam, including federal CANSPAM Act) and see Chapter 12 generally (Privacy) and Chapter 12.19 (Sharing of Information for Unsolicited Marketing).
- 11 The Rules Amendments and Committee Notes concerning electronically stored information can be found at the following location: [http://www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf).
- 12 See 15 U.S.C. § 1681c(g)(1) (added by the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”) (15 U.S.C. §1601 et seq.), which amended the Fair Credit Reporting Act (“FCRA”).  
or transaction.” (the “Truncation Requirements”). 15 U.S.C. § 1681c (g)(1).