

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

Guide to Computer Law—Number 290

## 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.

## Let's Play "Name that Security Violation!"

The idea of requiring security protections for data relating to individuals is now upon us, but its scope is often unknown and perhaps unknowable by ordinary businesses. To test your knowledge, take the following quiz:

*Which of the following information security practices are against the law? Assume that the information involved is: consumer buyer's name, credit or debit card number, and expiration date; check number, routing and account number, and driver's license number ("Info"). For extra points, name the statute or court case establishing the law violated:*

- (1) storing the Info in multiple files when there is no longer a business need to keep it;
- (2) failing to use readily available security measures to limit access to computer networks through wireless access points on the networks;
- (3) storing Info in unencrypted files that can be accessed easily by using a commonly known (within the company storing the Info) user ID and password;
- (4) failing to limit sufficiently the ability of computers on an in-store network to connect to computers on other in-store and corporate networks;
- (5) failing to employ sufficient measures to detect unauthorized access, such that a hacker could use the wireless access points on one in-store computer network to connect to, and access Info on, other in-store and corporate networks;
- (6) failing to encrypt Info while in transit or when stored on in-store computer networks;
- (7) storing the Info in files that can be accessed "anonymously" (pretending that "anonymous" means using a commonly known default user id and password);
- (8) not using readily available security measures to limit access to one's computer networks through wireless access points on the networks;
- (9) failing to employ sufficient measures to detect unauthorized access or conduct security investigations; and
- (10) creating unnecessary risks to the Info by storing it for up to 30 days when the storing company no longer has a business need to keep it, and in violation of bank rules (and that as a result, a hacker could use the wireless access points on an in-store computer network to connect to the network and, without authorization, access network Info).

Circle each item that violates the law: 1 2 3 4 5 6 7 8 9 10.

For the extra points, list the applicable statute, regulation or court case:

**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.

\_\_\_\_\_.

If you circled either (1) through (5) or (6) through (10) you would be right, at least according to the Federal Trade Commission (FTC). If you listed a statute, regulation or court case setting out an obligation regarding any express item, you would be wrong. Why? Because there are none.

If you circled some items but not others because you thought of situations in which the behavior would be reasonable, you would be right. And that is a problem: one cannot conform behavior to legal requirements until one knows what those requirements are. This premise, however, assumes that a legal requirement exists; that is not the case for security obligations for all U.S. companies in all circumstances or even for the Info, notwithstanding the seemingly contrary position of the FTC. When a legal obligation does exist, the rules vary. And if the requirement is a general rule such as for “reasonable” behavior or “fairness,” the required behaviors will necessarily shift with circumstances and subject matter so, again, a detailed list like that set out above is not automatically meaningful.

The above list comes from two recent FTC enforcement actions, both settled by consent orders without litigation. The FTC alleged, respectively, that (1) through (5), and (6) through (10), constituted a “failure to employ reasonable and appropriate security measures to protect personal information and files [that] 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 and is an unfair act or practice.” Because of how the cases ended, we do not know whether the FTC was right or wrong in concluding that an unfair practice occurred. We do know that, using a general deceptive and unfair practices statute, the FTC seems to have found a heretofore unknown, federal, general obligation to maintain security for personally identifiable data. The two actions are *In the Matter of DSW Inc.*, File No. 052 3096 (Dec. 2005) (items 1-5) and *BJ’s Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 2005) (items 6-10). To suddenly create and enforce a list in hindsight as the FTC apparently did, is to govern more by the concept of “shock and awe” than by publicly considered and published public policy.

Because the actions were settled, no court will examine the list or determine whether, under principles of due process and the like, appropriate notice was provided of an actual compliance obligation or whether imposing security obligations under this statute exceeds FTC powers.

Security obligations of the type discussed here are emerging from various sources. Irrespective of statutory or case law it is prudent today to take care of information even if such is not legally required. Also, certain federal laws generally require reasonable care or the like to be taken by certain companies. See *e.g.*, the federal *Gramm Leach Bliley Act* re certain consumer information held by defined “financial institutions,” and the federal *Health Insurance Portability and Accountability Act*

*of 1996* re security obligations of health care providers and others within the law’s scope. Also a few states, such as California, impose a general security obligation with respect to defined “personal information” regarding CA residents.

Moreover, in some private contracts, such as “merchant agreements” between a retailer and the processor to whom the retailer turns in customer credit or debit card “slips,” a merchant must take certain security measures and card association rules require or encourage the bank or processors to so contract. But at least one state, Washington, has invalidated part of those merchant agreements as void against public policy when they prevent retailers from trying to obtain enough information to know with whom the merchant is dealing.

The Washington action illustrates another thing that is wrong with the FTC’s list. Even had the details been the subject of public notice, some of the items on the list are wrong or at least questionable. The FTC assumes that a “violation of bank rules” justifies viewing the violation as an “unfair act or practice.” But the rules that appear to be at issue are the ones set forth in the merchant agreement between the credit card processor and a retailer (BJ’s), a private contract. Further, it is some of those very rules that at least one state—Washington—views as void against public policy:

[T]he legislature finds that some retailers are deterred from verifying their customers’ identity *by contractual arrangements with credit card issuers*. The legislature declares that such contracts violate the public policy that all citizens should be able to take reasonable steps to prevent themselves and their communities from falling victim to crime.<sup>1</sup>

(1) Any provision of a contract between a merchant or retailer and a credit or debit card issuer, financial institution, or other person that prohibits the merchant or retailer from verifying the identity of a customer who offers to pay for goods or services with a credit or debit card by requiring or requesting that the customer present additional identification is void for violation of public policy.<sup>2</sup>

Is Washington right in taking this action? California law would say no—California prohibits merchants from taking and/or recording certain verification steps<sup>3</sup> But my point concerns not who is right or wrong—the point is that the varying approaches illustrate that little is commonly known or agreed in this new area of information security and fraud prevention. Thus, the FTC’s list assumes the existence of a level of obviousness and transparency that does not exist.

Parts of the FTC’s list are simply wrong. Look at the allegation that BJ’s “created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business

need to keep the information, and in violation of bank rules.” There was a business need to keep at least part of the Info. For one thing, the federal Truth in Lending Act (12 CFR § 226.13) gives a credit card holder 60 days to dispute a transaction and gives the card issuer another 90 days to investigate it and make a reasonable determination regarding the validity of the transaction. This investigation is done by contacting the retailer and making it supply, essentially, proof that the transaction occurred with the cardholder. The issuer conducting the investigation might determine to side with the cardholder and that will initially relieve the cardholder of the repayment obligation. But that is not necessarily the end of it. If the retailer does not agree with that determination, the retailer can take it all up in court. How long does a court action take? Several years in most states.

In short, there is a business need to keep Info for more than 30 days. BJ’s might have contracted for a shorter period with its card processor, but likely not as to *all* Info (*e.g.*, the merchant agreement likely prohibited BJ’s from keeping the actual credit card number). If BJ’s did so contract, or if “bank rules” required BJ’s to do so, the Washington legislature would have it right: how can fraud be prevented if insufficient information about transactions may be retained in order to prove the transaction when other rules require or allow such proof? A potential collision exists between public policies regarding the need to prevent identity theft and fraud on the one hand, and to protect individual data on the other; this is a train wreck waiting to happen and simplistic lists are not helpful. A complex balancing of competing public policies will be required to achieve any reasoned outcome.<sup>4</sup>

For example, the European Union recently amended a directive<sup>5</sup> to require telecommunication companies to retain certain customer data for period of time *longer* (appx. 6 months to 2 years) than the data was commonly being retained by companies trying to comply with a countervailing, general “don’t keep information too long” concept in EU law. Law enforcement authorities were concerned that data was being discarded too quickly for them to deal with crime or terrorism. In short, public policies and reasonable minds differed as to what was a reasonable time to keep the information. Yet the FTC implies that answers are obvious. They are not.

Still, the list is an important indication of what the FTC thinks is required to avoid unfair acts or practices. Accordingly, businesses with Info may wish to consider and test compliance with the list and give some thought to what will be on the next list.

That can be the subject of our next guessing game.

#### ENDNOTES

<sup>1</sup> WA Leg. 2003 c 89 § 1.

<sup>2</sup> RCW 19.192.020(2003).

<sup>3</sup> See CA Civ. Code § 1747.8.

<sup>4</sup> For a discussion of this potential collision, see Raymond T. Nimmer and Holly K. Towle, *The Law of Electronic Commercial Transactions* (A.S. Pratt & Sons, 2003) at Chapter 15.06[1][b]

<sup>5</sup> See *e.g.*, Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC {SEC(2005) 1131}