

CCH[®] GUIDE TO COMPUTER LAW

Guide to Computer Law—Number 285

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.

Information Security Breach Notification Statutes

Question: What state laws have been enacted in the last year that may increasingly impact every business holding information electronically (*i.e.*, computer information)?

Answer: Statutes in at least ten states now require notice upon a breach of the business' information security when electronic, "personal information" is exposed.

These statutes follow, but also diverge from, a California statute enacted in 2002. This column discusses these statutes as well as federal guidance. The primary focus of these rules is on electronic information, but some also pertain to any covered information, no matter its form.

Background

California started it. It enacted Cal. Civ. Code §§ 1798.82 and 1798.29 which, respectively, apply to state agencies, or businesses or persons conducting business in California. With significant ambiguities, the CA statute essentially provides that a business owning or licensing "personal information" must disclose any security breach of its computer system "to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." If someone else owns the data (*e.g.*, the business is processing or hosting data for another), then the business suffering the security breach notifies the owner of the data. The intention is to warn those whose data may have been compromised so they can take appropriate steps to protect their own interests.

Everyone has likely seen reports of notices given recently by various businesses suffering security breaches: Choicepoint, Bank of America, CitiFinancial, and so on. The California statute was premised on the assumption that electronic "hacking" posed the greatest threat. Not surprisingly, that assumption is not necessarily correct (*e.g.*, a 2005 follow-up to a 2003 FTC report confirms that identity theft, for example, is more likely to come from persons the victim knows such as family members and relatives, and that "Although there has been much recent public concern over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels"). If incidents creating the need for notice are actually examined, hacking is a cause but so are errant employees, failures in physical security, and failures by service providers (*e.g.*, provider loses tape containing computer information).

Regardless, the statutes place costly compliance obligations on businesses. The obvious value of the statutes is that potential victims of identity theft can take protective action once they become aware that their information may be at risk. On the other hand, the cure contemplated by the statutes may exacerbate the problem.

This has already started to happen: scam artists hear about the security breaches too and then, such as in a phishing email, offer to “help” the consumer with the breach once the consumer provides authenticating information (which the scamster uses to engage in actual identity theft).¹

Be that as it may, this legislative train is rolling and more states are getting on board (10 and still counting). Accordingly, businesses that do not already have a response plan in place may wish to establish one; businesses with an existing plan should review and broaden it in light of the new statutes.

Scope

The scope of the statutes is often unclear because most turn on data ownership or other rights. For example, the

California statute applies to “[a]ny person or business that conducts business in California, *and that owns or licenses computerized data* that includes personal information.” The problem is that no intellectual property law regime, other than perhaps trade secret law, grants ownership in mere data. So at the outset, one can legitimately wonder who “owns or licenses” the particular data.

Non-Uniformity

These statutes are not uniform. Compliance, therefore, requires review of each one that applies. For example, some of the statutes cover every person or business given a particular tie to the state, while others only cover data or information brokers or collectors (variously defined), and others cover state agencies.

Personal Information

Generally, the kind of information that triggers a need to provide notice is “personal information” that has been exposed to a security breach. But non-uniformity and exceptions exist in what constitutes “personal information.” The following comparison is illustrative of the problem:

California	Georgia	Montana	North Dakota
<p>An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:</p> <p>(1) Social security number;</p> <p>(2) Driver’s license number or California Identification Card number;</p> <p>(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>[Essentially same as CA through §(2)]</p> <p>(3) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;</p> <p>(4) Account passwords or personal identification numbers or other access codes; or</p> <p>(5) Any of the items contained in subparagraphs (1) through (5) of this paragraph when not in connection with the individual’s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.</p>	<p>An individual’s name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual’s passport number, driver’s license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to obtain access to the individual’s finances, or any other financial information as provided by rule. A social security number, in and of itself, constitutes personal information.</p>	<p>[Essentially same as CA through §(2)]</p> <p>(3) A nondriver color photo identification card number assigned to the individual by the department of transportation ...</p> <p>(4) The individual’s financial institution account number, credit card number, or debit card number in combination with any required security code, access code or password that would permit access to an individual’s financial accounts;</p> <p>(5) The individual’s date of birth;</p> <p>(6) The maiden name of the individual’s mother;</p> <p>(7) An identification number assigned to the individual by the individual’s employer; or</p> <p>(8) The individual’s digitized or other electronic signature.</p>

The differences in these definitions lead to complexities and significant costs, including legal and programming. There are also dormant commerce clause constitutional questions as conflicting statutory regulations continue to be enacted.

But the immediate practical effect for businesses with a multi-state customer base involves developing a legally compliant multi-state approach. For example, the statutes affect the manner in which businesses may wish to maintain their data files. Most require a "combination" of information (subject to exceptions) such as the individual's name with another data element, in order for the aggregate to qualify as "personal information." Thus, one method of falling outside coverage of the statute is to prevent the combination from occurring, *i.e.*, break up the combination or take other steps so that the statutory definition is not triggered (this also serves the salutary purpose of making it harder for an unauthorized person to associate the data elements). Thus, if a business combined my name and social security number, instead of putting "Holly Towle" and my SSN in the same unencrypted database, it could encrypt one of those elements. Similarly, some businesses fall outside coverage because they do not have the required combination in the first place, *e.g.*, a business might have my name but not another required data element.

Many businesses already incurred the expense of taking the kinds of steps discussed above in 2002 when the California statute was enacted. But now they will have to do it again. *The new statutes add additional data elements and different rules for some of those elements.* Montana, for example, says that a social security number "in and of itself, constitutes personal information," so if in the above example the programming had encrypted my name to break up the combination of name and SSN, that won't work in Montana. North Dakota says that a birth date can be a relevant data element. If a business holding names and birth dates previously concluded that it did not hold "personal information" under the CA statute, the business would still be right for CA but wrong for ND.

Federal Guidance for Gramm Leach Bliley Financial Institutions

The state statutes are not all the law there is on this topic. "Financial Institutions" ("FI") are required by the federal Gramm Leach Bliley Act to provide information security. The term FI is misleading because it connotes banks and the like, when in fact, it covers a large range of other businesses that do not realize they are FIs. There are several regulators, including the banking regulators, the SEC and the FTC. In 2005 the banking regulators issued guidance regarding when FIs subject to their jurisdiction are required to give notice of an information security breach.

The guidance directs FIs to implement a response program tailored to the size, complexity, and nature of their own operations, including contracts with service providers requiring them to provide security as well. One of the ambiguities in most of the state statutes is whether federal consumer disclosure rules under the Electronic Signatures in Global and National Commerce Act must be met before sending notice by email. The federal guidance gives a clear answer, "no," as to its rules. Unlike the state statutes, the guidance also acknowledges that notice is not always warranted. Additionally, the guidance confines coverage to "sensitive customer information," *i.e.*, information that could result in substantial harm or inconvenience to a customer. The state statutes get close to this in their "combination" concept because some of the combinations tend to indicate sensitive data as combined. But they tend not to pick up other nuances (such as the "warranted" notice concept, but exceptions exist). Conversely, and unlike most of the state statutes, the federal guidance does not contain an exclusion for encrypted information. This means, for example, that if a business previously incurred the expense and operational complexities of encrypting data in order to comply with the CA statute, that encryption could be irrelevant if the business is an FI. The encryption will still be helpful, but not determinative under the guidance, so another compliance review may be advisable.

Much more needs to be said about these statutes but space (and reader patience) does not allow. Steps can be taken to ease compliance, however, so review is advisable.