U.S. Data Privacy Regulation:

State Legislation, Federal Preemption and Operational Challenges for Service Providers

September 15, 2006

Jonathan B. Wilson and C. Celeste Creswell

Presented October 20, 2006
Edison Electric Institute
Santa Fe, New Mexico

Table of Contents

About the Authors

Jonathan B. Wilson is Senior Vice President, Legal and Corporate Development, for Web.com, Inc. (NASDAQ: WWWW), the leading destination for the simplest yet most powerful solutions for websites and web services. Mr. Wilson is also the Chair of the Internet Industry Committee for the ABA's Public Utility, Communications and Transportation Law Section and has served in that capacity since founding the committee in 1997. Mr. Wilson is the author of *Out of Balance: Prescriptions for Reforming the American Litigation System* (iUniverse, 2005) and co-authored and co-edited *Internet Forms and Commentary: A Practitioner's Guide to E-Commerce Contracts and the World Wide Web* (American Bar Association: 2003). He earned his J.D. from George Washington University in 1991 and was graduated Phi Beta Kappa from William and Mary in 1988.

C. Celeste Creswell is a partner in the Atlanta firm of Wargo & French, LLP where she maintains a practice focusing on commercial and complex litigation with an emphasis on cases involving the Internet and e-Commerce. Ms. Creswell is Vice-Chair of the Internet Industry Committee for the ABA's Public Utility, Communications and Transportation Law Section. She earned her J.D. magna cum laude in 1996 from the University of Georgia where she was Executive Notes Editor of the Georgia Law Review and was inducted into the Order of the Coif. She earned a B.S., summa cum laude, in Decision Science (Mathematics, Computer Science, Business Economics) from Berry College. From 1996 to 1998 she clerked for the Honorable Curtis L. Collier, U.S. District Court (E.D. Tenn.).

PART I DATA PRIVACY IN THE NEWS

In the past few years there have been numerous news reports regarding data theft and identity theft. Among the most notable of these incidents was the ChoicePoint fraud, which compromised the personal records of more than 163,000 consumers, resulted in at least 800 cases of identify theft, and led to the largest civil penalty in Federal Trade Commission history.[1] On January 26, 2006, the FTC announced a settlement with ChoicePoint that required the company to pay $10 million in civil penalties and $5 million in consumer redress.[2] The settlement also requires ChoicePoint to "establish and maintain reasonable procedures to ensure that consumer reports are provided only to those with a permissible purpose" and to have those procedures audited every 2 years for the next 20 years.[3]

More recently, in May 2006, the U.S. Department of Veterans Affairs announced than an employee had compromised the names, social security numbers and birth dates of more than 26 million U.S. veterans when the employee took home a disc containing unencrypted data only to lose the disc in a home burglary.[4] While the hard disc containing the data was recovered within 60 days of its compromise, and the Department of Veterans Affairs has announced that it is "highly confident" the data was never accessed, for almost three months the incident played out in news reports and doubtless consumed time and efforts on the part of law enforcement and Department administrators.

---

[1] *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006, *available online at* www.ftc.gov/opa/2006/01/choicepoint.htm.
[2] *Id.*
[3] *Id.*
[4] Department of Veterans Affairs Website; http://www1.va.gov/opa/data/data.asp.

While some might conclude that the prevalence of such news reports suggests data ***theft*** is on the rise, the prevalence of the stories could also be the result of new state laws requiring ***disclosure*** of security breaches involving specific terms of personal data. California enacted the first state law requiring such notification, and at least twenty (20) states have since done the same. These state laws differ significantly and, in some instances, may impose conflicting obligations on companies operating in multiple states. Congress is considering several pieces of legislation that could preempt these myriad state acts, bringing added uniformity but possibly increasing the compliance burden. To understand the relationship between state and federal legislation in this context requires consideration of the underlying security threat that prompted California to enact the first disclosure law, the conflicting requirements of the state laws enacted in response to this threat, and the potential impact of new federal legislation.

Policy makers are concerned with the security and integrity of personal data and personal financial data because of the impact compromised data can have on protecting bank account information, ensuring the integrity of credit card purchases, protecting executive travel itineraries and maintaining the confidentiality of prescription drug histories. In addition because certain kinds of personal data can be used to access private databases, there is virtually no limit to the kind and type of damage that can be done to an individual and that individual's credit history if personal financial data is compromised by a perpetrator intent on causing damage. Spurred on by recent publicity, consumer fears of identity theft and security breaches cost web-based businesses substantial lost business opportunities. The Gartner Group estimates that 86 percent of American adults

refrain from doing business on the Internet because of security concerns[5] and that concerns over privacy, security, and fraud have prevented consumers from utilizing the Internet for online bill payment.[6]

Some experts have claimed that network intrusions have quadrupled in the past few years.[7] Despite the criminal sanctions and serious consequences that already attach to vandalizing websites, hacking and other kinds of Web vandalism persist with cult-like devotion. In February 2004, 8 million credit card numbers were accessed by hackers who attacked DPI, a payment-processing company that handles transactions for VISA, MasterCard, Discover, and American Express. Soon thereafter, hackers worked for hours in a loosely coordinated competition to win a "contest" by vandalizing Internet sites and tallying the most points.[8] Aggressive law enforcement efforts directed toward hackers seemed to have little impact on the number of network intrusions.

Companies that are victimized in such incidents often wrestle with the decision of whether to disclose a security breach and its potential ramifications to consumers whose private data may have been compromised.[9] Advocates of disclosure argue that immediate notification minimizes the risk of harm from the attack as affected individuals can place holds on their accounts and take other measures. Disclosure further aids the investigation of an attack and may thwart future attacks by the same perpetrator. Others express concern that disclosure raises a red flag for potential hackers by identifying system vulnerabilities before they can be resolved. Disclosure may also result in

[5] Tusecure Corp., Information Security, Sept. 2001 (on file with authors).
[6] Federal Reserve Bank of Chicago, Economic Perspectives (Dec. 2001).
[7] Robert A. Clyde, *Guarding Against Network Security Attacks*, J. Counterterrorism & Homeland Sec. Int'l (Winter 2003).
[8] Ted Bridis, Hackers Limit Disruption to Small Internet Sites, WASH. POST, July 7, 2003.
[9] Katie Hafner & John Biggs, *In Net Attacks, Defining the Right to Know*, N.Y. Times (Jan. 30, 2003).

consumer-initiated class action litigation[10] that exposes companies to the expense of civil litigation even though no actual harm may have resulted from the security breach. In addition, from a practical perspective, executive decision-makers are often forced to consider these competing priorities in a crisis atmosphere where information is limited and events are still unfolding. Those executives must balance compliance concerns with risk mitigation, public relations and shareholder value concerns with little time and less than complete information. Data security and the threat of compromise is a significant risk for enterprises that maintain databases of personal or consumer information and there is no easy solution to mitigate that risk.

[10] *See, e.g., Lawsuit Accuses Tri-West Health Care of Negligence*, Ariz. Repub., Jan. 30, 2003 (class action filed in Arizona after computer files and data files containing personal information stolen).

PART II STATE REGULATION OF DATA PRIVACY

In response to hackers gaining access to the state of California's payroll database that contained personal and financial information about the state's 265,000 employees, California adopted a law requiring companies doing business in California and state agencies to disclose publicly any computer security breaches that involve the personal information of a California resident.[11] California's disclosure law protects consumers against identity theft and credit card fraud by requiring quick disclosure of any breach in the security of a data system when the hacked information is personal and was not encrypted.

The California disclosure law requires disclosure of any security breach to each affected resident in California—regardless of where the disclosing company is located or where the security breach occurred—whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The Act defines "personal information" as an individual's first name or initial and last name in combination with one or more of the following "data elements," where either the name or the data element(s) is not encrypted:

- Social Security number
- Driver's license number or California ID number
- Account number or debit or credit number in combination with any required security code, access code, or password that would permit access to a person's financial account.[12]

[11] Cal. Civ. Code § 1798.82 (West 2003).
[12] Cal. Civ. Code § 1798.82(e) (2003).

The Act excludes encrypted data from its definition of personal information yet does not include a definition of what encryption means or what type of encryption is sufficient (certain methods of encryption offer only limited protection against a security breach).

Any unauthorized acquisition of computerized data constitutes a security breach under the Act as long as it compromises the "security confidentiality" or integrity of the information. This includes more than attacks on networks by hackers. For example, disclosure may be required in the event computer hard drives or disks that contain personal information are stolen. Several recent, highly publicized thefts of computer hard drives resulted in the disclosure of thousands of names and Social Security numbers. Under the new law, had any of those individuals whose personal information was stolen been California residents, disclosure would have been mandatory.

Because victims of identity theft will wish to act quickly to minimize damage, the law requires that notice be made "in the most expedient time possible" and "without unreasonable delay." The need for speed is tempered by the requirements of law enforcement. The California law requires that any disclosure of the security breach be "consistent with the legitimate needs of law enforcement" and with the time necessary to restore "reasonable integrity" to the affected data system. This encourages companies to report security breaches to law enforcement while they decide whether and when to notify consumers.

Failure to provide prompt notice may expose a company to a suit for damages. The Act provides that consumers who have been injured by a violation of the law may bring a civil action for damages. Claims under the Act also may be accompanied by claims of unfair business practices under state law or misrepresentation claims premised

on violations of company privacy policies ensuring protection of consumer data. Notably, ChoicePoint claimed it delayed disclosure in order to avoid impeding ongoing criminal investigations, but ultimately agreed to a $15 million settlement of the FTC claims rooted in such delayed disclosure.

Other States Enact Similar But Conflicting Legislation

At least twenty states have enacted legislation similar to California SB 1386, but many of those laws differ in material respects.[13] For example:

- Georgia's statute[14] regulates only "information brokers" (i.e., companies that maintain personal information "for the primary purpose of furnishing personal information to nonaffiliated third parties"), but it broadly defines "personal information" to include information that if "compromised would be sufficient to perform or attempt to perform identity theft."[15]
- Nevada and North Carolina require notification of data theft even if the stolen data is encrypted.[16]
- Illinois does not allow delay in notification even if the delay would aid law enforcement efforts to pursue the person who stole the information at issue.[17]

Appendix A provides a list of significant information security laws and cases, including a list of state laws mandating disclosure of security breaches. Given the absence of a uniform act governing notice of data theft, questions such as whether, when, to whom,

[13] Behnam Dayanim and Kristine Rembach, *Notice of Data Theft: States and the Congress Jump on the California Bandwagon*, 38 Sec. & Comm. Reg. 22, 281, 283 (Dec. 21, 2005).
[14] Georgia Senate Bill 230 (2005).
[15] *Id.*
[16] Nevada Assembly Bill 334 (2005); Nevada Senate Bill 347 (2005); North Carolina House Bill 1248 (2005).
[17] Illinois, H.B. 1633 (2005).

and in what manner security breaches must be reported may only be answered by reference to the law of each applicable state.

The Domestic Compliance Conundrum

The myriad state acts described above create an interesting dilemma for multistate enterprises.[18] In the unfortunate event of a security breach, should a company discretely notify only its customers who live in states with mandated disclosure? Consumer advocates argue for full disclosure to all customers, even in the absence of an applicable state law. What if there is an ongoing criminal investigation that prohibits disclosure in one state but a neighboring state's law mandates disclosure? Anticipation of such quandaries, compounded by the ever increasing number of inconsistent state statutes, has given rise to a call for uniform federal regulation.

[18] Although the disclosure obligations of the state laws impose new duties, companies that post privacy policies or are subject to privacy laws have been required to employ security measures to prevent, detect, and monitor intrusions for some time now. The FTC has aggressively targeted companies that fail to encrypt personal information properly although they have promised consumers they have done so. *See Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security* (June 18, 2003), available at www.ftc.gov/opa/2003/06/guess.htm; *see also FTC Targets Security to Combat Identity Theft* (Apr. 3, 2003), available at www.ftc.gov/opa/2003/04/idttestimony.htm; *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises* (Aug. 8, 2002), available at www.ftc.gov/opa/2002/08/microsoft.htm; *Eli Lilly Settles FTC Charges Concerning Security Breach* (Jan. 18, 2002), available at www.ftc.gov/opa/2002/01/elililly.htm. A close reading of FTC complaints reveals a standard of care requiring storage of consumer information in an "unreadable, encrypted format at all times," and the implementation of procedures that ensure compliance not only with company privacy policies but also with "reasonably foreseeable vulnerabilities in their website and computer networks." *Id.* Indeed, failure to deploy antiworm patches to protect networks against attack has been found to be unreasonable in certain circumstances. *See* 4 Computer Tech. Law Rep. 12 (BNA) (June 20, 2003). FTC settlements in recent cases where posted privacy policies were breached further reveal the need to update written security policies, periodically monitor for risks, and train employees on how to identify and manage security breaches. *Id.* Settlements in privacy and security cases pursued by state attorneys general suggest the need for immediate action to suspend activities impacted by a security breach, to investigate the cause of such an incident, and to take whatever remedial action may be warranted.

Worldwide Implications

However complicated the problem of compliance in the U.S., it is far more difficult for service providers that have operations in the European Union or that are otherwise subject to jurisdiction in an EU member country. Data security is a special concern in Europe and, in 1995 the Council of Europe adopted a directive that ordered member steps to adopt national legislation that would secure the privacy of certain types of personal information of EU citizens. Among other things, the EU Data Privacy Directive forbids EU citizens and business from transferring personal data outside the EU except to nations that have what the EU considers adequate safeguards for data privacy. Perhaps not surprisingly, the EU does not consider U.S. protections on data privacy "adequate." Although the national rules only apply to businesses subject to national jurisdiction, they can extend to U.S. firms if those firms have operations in the EU or if those firms maintain databases (even outside the EU) that contain data of EU citizens.

Because of the potential extraterritorial effect of the EU Data Privacy Directive, U.S. firms that feared business disruption or loss of opportunities because of the perceived laxity in U.S. data privacy laws pressured the U.S. Department of Commerce to negotiate a "safe harbor" treaty with the U.S.[19] Under the U.S. safe harbor provisions, U.S. firms that register with the U.S. Department of Commerce and who meet the safe harbor's requirements of posting privacy notices and maintaining certain safeguards can collect and maintain personal information from EU citizens without violating the EU Data Privacy Directive. Satisfying the safe harbor requirements, however, is no easy task

[19] *See generally* http://www.export.gov/safeharbor/index.html.

and violations may trigger private rights of action, FTC enforcement under Section 5 of the FTC Act, and fines of up to $12,000 per day.[20]

PART III FEDERAL LEGISLATION ON DATA PRIVACY

Whether Congress will rescue multistate enterprises from conflicting state laws and satisfy EU concerns remains to be seen, but there are several bills pending before Congress that could preempt state law and create uniform compliance obligations. "Their sheer number presages the difficult questions of competing committee jurisdiction and variation in approach which the Congress must resolve if legislation is to be enacted. In each body, at least three committees claim jurisdiction and currently are considering measures."[21]

Of course, the price of uniformity may be even more costly compliance requirements. In this regard, one bill pending in Congress, the Identity Theft Protection Act, S. 1408, covers ***hard copy and*** electronic data and requires covered entities to develop effective security programs to protect the data, unlike many of the state acts.[22]

Notably, however, S. 1408 vests the FTC and state attorneys general with enforcement power and does not create a private right of action.[23] Similarly, the Personal Data Privacy and Security Act of 2005, S. 1789, creates no private right of action, instead vesting enforcement authority in the United States Attorney General and the state

[20] http://www.export.gov/safeharbor/sh_overview.html
[21] Dayanim and Rembach, *Notice of Data Theft: States and the Congress Jump on the California Bandwagon*, supra n. 11.
[22] *Id.* at 284-85.
[23] *Id.* at 285.

attorneys general.[24] Thus, although these federal proposals may increase the compliance burden, they may also remove the possibility of a class action.

These distinctions render the scope of preemption critical. Consider the following scenario: State A's act (which creates a private cause of action) is triggered by 500 disclosures of personal information and has no safe harbor for encrypted information; State B's Act (which also creates a private cause of action) is triggered by 1,000 disclosures but has a safe harbor for encrypted information; and the federal act (which does not permit a private cause of action) is triggered by 10,000 disclosures but preempts only state laws that regulate the same conduct it covers. A security breach compromises the personal information of 9,999 consumers. Because the preemption provision is limited and the conduct falls below the federal threshold, the covered entity could be subject to individual or class actions in State A (if at least 500 of the disclosures concerned residents of State A) or State B (if 1,000 of the disclosures concerned State B's citizens and the information was not encrypted).

Another contender is H.R. 3997, the Financial Data Protection Act of 2006. Until August 2006, H.R. 3997 seemed to have a fair chance of passing. Like S. 1408, H.R. 3997 would have pre-empted inconsistent state laws and adopted a national standard for financial data security and a national rule for the disclosure of security breaches. Passage of the bill seemed doomed, however, shortly before the August recess when "a jurisdictional dispute between two House committees with oversight of the issue" prevented the bill from coming to a vote.[25] Consumer groups including U.S. PIRG and

[24] *Id.*
[25] Congress Wades Into the Data Breach, Fulton Co. Daily Rpt., (Aug. 8, 2006) (M. Coyle) 1, 8.

Consumers Union have aligned against the measure and passage in a mid-term election year now seems doubtful.

Until there is federal legislation, the uncertainty, exposure, and proof problems suggested by the foregoing scenario will remain. Even after federal legislation is enacted, the scope of any preemption will likely be a hotly contested issue.

PART IV WHAT SERVICE PROVIDERS CAN DO

Service providers should, if they have not already, develop a comprehensive program for the maintenance of databases containing personally-identifiable information of the kind at issue in the broadest applicable state or federal statutes ("PII").

Assembling a Team

Like any other compliance project, a project to secure a service provider's PII should have executive sponsorship, to ensure the cooperation of the various teams within the company that will be affected. A data security project, much like the kind of compliance project entailed by Section 404 of the Sarbanes-Oxley Act, is interdepartmental. The IT Department typically will be responsible for the hardware and software systems that contain the PII, while the customer service organization often will be primarily responsible for the customer relationship management (or "CRM") software that utilizes the PII. While compliance may often be a function of the Legal or Compliance Departments, organizing a successful compliance project will require inter-departmental cooperation.

Many service providers will also want to involve outside experts. While there are IT consulting organizations that can take on an entire compliance project on an outsourced basis, the costs that complete outsourcing would entail are not always necessary. More often an outside expert can come in handy by identifying applicable laws, areas within the organization where attention may be needed, and by identifying common solutions for problems. The organization itself will want to have a sense of

ownership about the project and at least one executive in the organization should have ultimate responsibility for its success.

Taking Stock

As an initial step, the project should take an inventory of all the PII the organization obtains from its customers and other sources as well as an inventory of every database where that data is stored and every software application through which that data can be accessed on that relies upon that data. By mapping databases and types of PII to particular applications and software programs, the project managers will be able to visualize how the organization collects PII, how the organization stores PII and how the organization uses PII. By understanding these impacts, the project managers can assess the vulnerabilities of the organization's systems and applications and can identify the kinds of risks the organization faces.

Taking Control

After taking an inventory of the organization's PII, and its related systems and applications, and assessing the organization's vulnerabilities to different kinds of risks, the project managers should develop controls for the organization's systems and applications. Those controls may range from traditional IT security devices, like firewalls, data encryption, password protection and even limiting access by biometric controls in certain areas, to business-level solutions, including changing the way the organization collects, stores and uses PII.

Newcomers to the topic of data security may sometimes ask, “is it always necessary to encrypt personally identifiable data?” While encryption is a relatively powerful control when it comes to data security, it is not always mandatory. And, more importantly, encryption by itself is not a “magic bullet.” Unfortunately for service providers, there is no magic bullet than can ensure compliance. The only way is to conduct an appropriate review of systems and applications and to develop a suite of controls that are able to provide adequate assurances of security.

Testing , Re-Testing, and Re-Thinking

After the organization has developed and implemented controls, the compliance project managers should develop a plan for testing those controls on a periodic basis. Ideally, the tests should be performed by persons or organizations that are independent from those that implemented the controls, to ensure accountability. Through the executive sponsorship of the project, a group within the organization should have the primary responsibility of conducting those tests on a periodic basis and reporting the results up through the organization. Where test results reveal failures in implementation or failures in control design, the organization should have a team with responsibility for remediating those failures.

While periodic testing (perhaps quarterly) constitutes control, there should also be in place a process for a less frequent (perhaps annual) review of controls design and overall risk assessment. That more far-reaching review should include a review of applicable law (as the legal regime for data integrity compliance is very much in flux)

and the means for modifying the control environment, test plan and audit plan at the same time.

Mapping a Response

In addition, as part of the overall compliance project, the executive sponsor should develop a "response plan" for the possibility that the organization's data is compromised. While the purpose of the compliance plan is to reduce the likelihood of compromise, no system of controls can guarantee error-free operation or that an organization's systems will be impervious to a determined attack. The response plan should contemplate:

1. **Protocols for reporting, collecting and disseminating information**: Who should be alerted if a compromise is suspected? Who should take responsibility for investigating the matter? Who should take responsibility for preparing a public disclosure of the potential compromise?
2. **Protocols for declaring that a compromise has occurred**: Who will be responsible for the determination that a compromise has occurred? What level of certitude will be required to make that conclusion? (The level of certitude may depend upon the applicable law).
3. **Protocols for coordinating both internal and external communications**: Much of the internal and external communications can be choreographed in advance and will need to be coordinated as the internal investigation unfolds. By preparing talking points and FAQs in

advance the executive response team can save hours or even days in responding to an incident.

4. **Governmental and industry contact information**: Service providers who are subject to state-level regulation may already have regulatory contact points but there may be different protocols for potential data compromise issues. An emergency response plan should contemplate the need to communicate with regulators and perhaps include periodic meetings and updates with those entities before a compromise incident occurs.

From the point of view of a service provider organization, it might be preferable if there were a single federal law that provided crisp and clear guidance on the level of care required for collecting and storing PII and responding to a potential compromise. Our current patchwork of state laws makes the compliance effort more difficult for organizations that span several states. Nevertheless, a robust compliance program, combined with a thoughtful plan for how to respond in the event of a potential compromise, can significantly mitigate the risk of data loss and the risk of liability in the event of an incident.

Appendix A

Index to Data Privacy and Information Security Laws, Regulations and Resources

1. **Security Breach Notification Laws**

Arkansas	Ark. Code Ann. § 4-110-101 *et seq*.
California	Cal. Civ. Code § 1798.82
Connecticut	2005 Conn. Acts 148
Delaware	De. Code Ann. tit. 6, 12B-101 *et seq*.
Florida	Fla. Stat. Ann. § 817.5681
Georgia	Ga. Code Ann. § 10-1-910 *et seq*. (applies to information brokers only)
Illinois	815 Ill. Comp. Stat. 530/1 et seq.
Indiana	Ind. Code § 1. IC 4-1-10 (applies to state agencies only)
Louisiana	La. Rev. Stat. Ann. § 51:3071 *et seq*.
Maine	Me. Rev. Stat. Ann. tit. 10, § 1346 *et seq*. (applies to information brokers only)
Minnesota	Minn. Stat. § 325E.61 and § 609.891
Montana	Mont. Code Ann. § 30-14-1701 *et seq*.
Nevada	Nev. Rev. Stat. 52.18 *et. seq.*
New Jersey	A. 4001, 2005 Leg., 211th Sess. (N.J. 2005)
New York	N.Y. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 *et seq*.
Ohio	Ohio Rev. Code § 1349.19
Pennsylvania	S.B. 712
Rhode Island	R.I. Gen. Laws § 11-49.2-1 *et seq*.
Tennessee	Tenn. Code Ann. § 47-18-2107
Texas	Tex. Bus. & Com. Code Ann. § 48.001 *et seq*.
Utah	Utah Code Ann. § 13-44-102 et seq.
Washington	Wash. Rev. Code § 19.255.010
Wisconsin	Wis. Stat. Ann. § 895.507

2. **Federal Statutes Regarding PII**

COPPA: Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 *et seq*. COPPA restricts the ability of website proprietors to collect certain kinds of personally-identifiable information from minors.

E-SIGN: Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001(d). E-SIGN provides for the enforceability of electronic signatures in interstate commerce.

FISMA: Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541-3549.

GLB Act: Gramm-Leach-Bliley Act, Public L. 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805. GLB imposes certain obligations regarding the collection, storage and use of personally-identifiable information on banks, bank holding companies and certain types of financial institutions.

HIPAA: Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320d-2 and 1320d-4. HIPAA imposes data security obligations on certain types of entities that collect, store and maintain personally identifiable information in connection with the provision of health insurance, health insurance benefits and medical services.

Homeland Security Act: Homeland Security Act of 2002, 44 U.S.C. § 3532(b)(1).

Sarbanes-Oxley Act: Sarbanes-Oxley Act, Pub. L. 107-204, Sections 302 and 404, 15 U.S.C. Sections 7241 and 7262. By requiring publicly-traded companies in the U.S. to make certain certifications in their public financial statements, including certifications regarding the presence of internal controls, this legislation implies a certain level of data integrity and system security with respect to entities subject to it.

Federal Rule of Evidence 901(a): see *American Express v. Vinhnee*, 2005 Bankr. LEXIS 2602 (9th Cir. Bk. App. Panel, 2005).

3. Statutes - State

1. **UETA:** Uniform Electronic Transaction Act, § 12 (now enacted in 46 states).
2. **Personal Information Security Statutes:** Ark. Code Section 4-110-104(b); Cal. Civil Code Section 1798.81.5(b); 52 Nev. Rev. Stat. Section 23(1); R.I. Stat. 11-49.2-2(2) and (3).

4. Regulations - Federal

1. **COPPA Regulations:** 16 C.F.R. 312.8.
2. **FDA Regulations:** 21 C.F.R. Part 11.
3. **GLB Security Breach Notification Rule:** *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision).

4. **GLB Security Regulations:** *Interagency Guidelines Establishing Standards for Safeguarding Consumer Information* (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision).
5. **GLB Security Regulations (FTC):** *FTC Safeguards Rule* (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 16 C.F.R. Part 314 (FTC).
6. **HIPAA Security Regulations:** *Final HIPAA Security Regulations*, 45 C.F.R. Part 164.
7. **IRS Regulations:** Rev. Proc. 97–22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.
8. **IRS Regulations:** IRS Announcement 98-27, 1998-15 I.R.B. 30, and Tax Regs. 26 C.F.R. § 1.1441-1(e)(4)(iv).
9. **SEC Regulations:** 17 C.F.R. 240.17a-4, and 17 C.F.R. 257.1(e)(3).

5. Regulations - State

1. **NAIC Model Regulations:** National Association of Insurance Commissioners, Standards for Safeguarding Consumer Information, Model Regulation

6. Court Decisions

1. *Bell v. Michigan Council 25*, No. 246684, 2005 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005) (Unpublished opinion)
2. *Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006)

7. FTC Decisions and Consent Decrees

1. In the Matter of CardSystems Solutions, Inc., (Agreement containing Consent Order, FTC File No. 052 3148, February 23, 2006), *available at* www.ftc.gov/opa/2006/02/cardsystems_r.htm
2. *United States v. ChoicePoint, Inc.* (Stipulated Final Judgment, FTC File No. 052 3069, N.D. Ga. January 26, 2006), available at http://www.ftc.gov/os/caselist/choicepoint/choicepoint.htm.
3. *In the Matter of DSW Inc.*, (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), available at www.ftc.gov/opa/2005/12/dsw.htm.

4. *In the Matter of BJ's Wholesale Club, Inc.* (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), available at www.ftc.gov/opa/2005/06/bjswholesale.htm.

5. *In the Matter of Sunbelt Lending Services, Inc.* (Agreement containing Consent Order, FTC File No. 042 3153, November 16, 2004), available at www.ftc.gov/os/caselist/0423153/04231513.htm.

6. *In the Matter of Petco Animal Supplies, Inc.* (Agreement containing Consent Order, FTC File No. 042 3153, November 7, 2004), available at www.ftc.gov/os/caselist/0323221/0323221.htm.

7. *In the Matter of MTS, Inc., d/b/a Tower records/Books/Video* (Agreement containing Consent Order, FTC File No. 032-3209, April 21, 2004), available at www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf.

8. *In the matter of Guess?, Inc*. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), available at www.ftc.gov/os/2003/06/guessagree.htm.

9. *FTC V. Microsoft* (Consent Decree, August 7, 2002); available at www.ftc.gov/os/2002/08/microsoftagree.pdf

10. *In the Matter of Eli Lilly and Company*, (Decision and Order, FTC Docket No. C-4047, May 8, 2002); available at www.ftc.gov/os/2002/05/elililly do.htm

8. State Attorneys General Consent Decrees

1. *In the Matter of Barnes & Noble.com, LLC* (Attorney General of New York, Assurance of Discontinuance, April 20, 2004); available at www.bakerinfo.com/ecommerce/barnes-noble.pdf.

2. *In the Matter of Ziff Davis Media Inc*. (Attorneys General of California, New York, and Vermont), Assurance of Discontinuance, August 28, 2002); available at www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf

9. European Union

1. **EU Data Protection Directive:** European Union Directive 95/46/EC of February 20, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Article 17, available at http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

2. **U.S. Department of Commerce Safe Harbor:** *See generally* http://www.export.gov/safeharbor/index.html