Washington Journal of Law, Technology & Arts

Volume 2 | Issue 4 Article 5

4-14-2006

Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide

Anthony D. Milewski Jr.

Constitutional & Regulatory
Cite as: Anthony D. Milewski Jr., *Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 Shidler J. L. Com. & Tech. 19 (Apr. 14, 2006), *at* <http://www.lctjournal.washington.edu/Vol2/a019Milewski.html>

COMPLIANCE WITH CALIFORNIA PRIVACY LAWS: FEDERAL LAW ALSO PROVIDES GUIDANCE TO BUSINESSES NATIONWIDE

Anthony D. Milewski Jr.[1]

Abstract

Over the past several years, personal information has been lost or stolen as a result of a series of high profile security breaches. In January 2006, the U.S. Federal Trade Commission announced that ChoicePoint will be required to pay $15 million in fines and penalties for a high profile security breach that occurred in 2005. The ChoicePoint breach and similar events have spurred an explosion of state and federal privacy legislation. In particular, the State of California has taken the lead by enacting the strictest disclosure and security procedure requirements in the country. The implications of California's new laws can be felt throughout the U.S. since they affect any business that collects personal information about California residents. This article will focus on a new California law, Assembly Bill 1950, which requires businesses to maintain "reasonable security standards" for personal information without further defining such standards. In particular, the article examines how businesses can comply with A.B. 1950 by performing a risk management analysis and borrowing security standards from the federal Gramm-Leach-Bliley and the Health Insurance Portability and Accountability Acts.

Table of Contents

INTRODUCTION

<1> Since the ChoicePoint security breach in February 2005, security lapses have compromised the personal information of more than 50 million Americans.[2] According to *The Economist*, data theft in America resulted in losses totaling nearly $50 billion in 2005.[3] In January 2006, the U.S. Federal Trade Commission levied $15 million in fines and penalties against ChoicePoint as a result of a high profile security breach that compromised the personal information of 145,000 U.S. residents.[4] To date, nearly 800 of the exposed individuals from ChoicePoint breaches have reported that some form of identity theft related crime has been committed against them.[5] As a result of such events, states are enacting new laws to protect personal information and businesses are scrambling to comply with these laws. Every state in America is now contemplating privacy legislation in some form or another.[6]

<2> The State of California has taken the lead by adopting new privacy laws with the country's most stringent requirements. A 2002 security breach of California's state web site, which compromised access to the Social Security numbers of all state employees, served as the impetus for the new laws.[7] Three laws characterize California's approach to privacy protection: Senate Bill 1386 (S.B. 1386),[8] Senate Bill 27 (S.B. 27),[9] and Assembly Bill 1950 (A.B. 1950).[10] This article briefly examines S.B. 1386 and S.B. 27 as precursors to A.B. 1950. The article then focuses on A.B. 1950's "reasonable security procedures" requirement and explains how businesses can comply with that law's ambiguous language by strategically borrowing security standards from the Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act ("HIPAA").

WHY IS CALIFORNIA'S PRIVACY LAW IMPORTANT TO YOUR BUSINESS?

<3> California's privacy laws reach far beyond the state's borders. As the tenth largest economy in the world,[11] nearly all of the nation's largest businesses work within the state and are therefore bound by its laws to some extent.[12] In addition, while the three laws discussed in this article are the first of their kind in the United States, several states, including New York, are considering similar measures.[13] Furthermore, the laws became even more influential following a June 2005 meeting of the National Association of Attorneys General. That group advised that, in the absence of conflicting local law, California's security breach notice requirement applies to residents of nearly every state.[14] Thus, understanding

how to comply with California law may help businesses satisfy future compliance requirements elsewhere in the United States.

OVERVIEW OF CALIFORNIA'S NEW PRIVACY LAWS

<4> California's new privacy laws impose three requirements on businesses that maintain personal information about one or more California residents in an electronic database. Businesses covered by the laws must notify California residents when the security of their personal information has been compromised[15] and when their information is shared with a third party.[16] In addition, businesses must maintain "reasonable security procedures" to protect personal information.[17]

<5> Senate Bill 1386, which took effect in July 2003, aimed to reduce the risk of theft of personal information maintained by persons or businesses in computer databases.[18] Senate Bill 1386 created strict requirements for notification of consumers following any breach of unencrypted personal data that includes an individual's name and credit card number, social security number, or driver's license number.[19] In addition, if prompt notice is not given to the consumer about a breach of personal information, S.B. 1386 provides a harmed customer with a private cause of action for damages and injunctive relief against the violating institution.[20]

<6> Senate Bill 27, the so-called "Shine the Light Law," took effect in January 2005.[21] It requires companies with customers in California to account to those customers, upon the customers' request, when they release personal information to third parties for marketing purposes.[22] All personal information shared with third parties within the twelve months prior to the request must be released to the requesting customer.[23]

<7> Assembly Bill 1950, which went into effect in January 2005, imposes a general security standard on businesses that maintain certain types of personal information about California residents.[24] Assembly Bill 1950 builds upon S.B. 1386 by not only requiring disclosure of security breaches that affect personal information, but also by requiring businesses to maintain "reasonable security procedures and practices."[25] Assembly Bill 1950's reasonableness requirement is discussed later in this article.

WHAT IS "PERSONAL INFORMATION" UNDER CALIFORNIA PRIVACY LAW?

<8> Of the three laws discussed, S.B. 27 takes the broadest approach to defining "personal information." S.B. 27 categorizes personal information into vast categories that make almost any information "personal" if it is not public and is attributable to an individual.[26] Under S.B. 27, upon a customer's request a business

will have to disclose the release of such information to third parties.

<9> By contrast, S.B. 1386 and A.B. 1950 define personal information more narrowly as an "individual's first name or first initial combined with any one or more data elements, when either the name or the data elements are not encrypted."[27] Assembly Bill 1950 defines these additional data elements to include a Social Security number, driver's license number, California identification card number, account number, medical information, or credit card or debit card numbers when combined with a code that would allow access to the underlying account.[28] Senate Bill 1386 similarly defines additional data elements; however, S.B. 1386 omits any reference to medical records. The omission of medical records from S.B. 1386 means that if an individual's name and medical records are released together, public disclosure may not be mandated. Furthermore, two of the three California laws have provisions which absolve a regulated entity from liability when the information released is already publicly available.[29]

WHAT DOES A.B. 1950 REQUIRE?

<10> Assembly Bill 1950 takes a bold approach to protect the personal information of California residents by encouraging "businesses that own or license personal information about Californians to provide **reasonable security** for that information."[30] In addition, the law provides that businesses that own or license personal information about California residents must "implement and maintain **reasonable security procedures**" appropriate to the nature of the information.[31] Assembly Bill 1950 requires a company, in addition to implementing reasonable security procedures, to also enter into contracts with its subcontractors requiring them to make the same commitment to "implement and maintain reasonable security procedures." [32] Since A.B. 1950 does not further define these reasonableness standards, it leaves businesses struggling to understand their scope and to implement business practices sufficient to avoid liability under A.B. 1950.

<11> Companies that are typically subject to A.B. 1950 are exempt from that statute's provisions when they comply with HIPAA, the California Financial Information Privacy Act, or any federal law that provides greater protection to personal information than A.B. 1950.[33] In other words, if a company that is not subject to HIPAA is wondering how it can best meet the ambiguous requirements of A.B. 1950, it can look to the HIPAA standards or standards imposed by other relevant federal laws such as the GLBA to inform its information policies.

<12> Thus, in order to avoid liability that might arise from failure to provide "reasonable security" under A.B. 1950, businesses should consider using HIPAA and the GLBA as guidelines for their own

security practices and procedures. Their decision to borrow from these laws and their associated regulations should be tempered by an individualized risk management strategy, since implementing unneeded procedures may cause businesses to waste valuable resources.

CONDUCTING A RISK ANALYSIS ASSESSMENT

<13> A business turning to HIPAA or GLBA standards for guidance on A.B. 1950 compliance should first conduct a risk analysis assessment as part of the process of borrowing standards. Such an assessment should be conducted using the following two-part risk management strategy.[34] The first step is a risk reduction strategy, whereby a company identifies threats and vulnerabilities to personal information. Once it has identified such threats and vulnerabilities, the business should rank and categorize them. Developing a hierarchy of risks allows a business to establish security procedures emphasizing the most pressing risks.[35] For example, in the banking industry, risks are typically categorized as legal, operational, reputational, and strategic.[36] Businesses should define categories relevant to the privacy goals of their specific industries.

<14> Next, the business must decide to handle identified risks in-house or subcontract a portion of them to third parties. [37] Transferring risk to another party should be considered by businesses that are unable to provide adequate security for personal information, if they can provide adequate security and also save money by outsourcing. Any decision to outsource, however, creates an ongoing duty to assess the performance of the party providing the security assurances. A business that has categorized its risks and assessed its data protection strengths and weaknesses, and decided not to outsource any of its identified risks, might find it helpful to borrow standards from GLBA or HIPAA in developing its internal security plan.

LOOKING TO FEDERAL REGULATIONS FOR GUIDANCE

<15> Businesses may look to both GLBA and HIPAA when creating policies and procedures that comply with A.B. 1950. Both regulations seek secure maintenance of consumer information and prevention of unauthorized use of the information inside or outside of businesses.[38] The primary differences in the regulations are industry-specific and do not reflect different approaches to protecting private information. For instance, GLBA explicitly requires that companies oversee that "service providers"[39] are protecting private information, while HIPAA more specifically requires "workforce"[40] compliance. The language in these two requirements is quite different; however, the general objective remains the same: businesses are responsible for protecting private information they

collect and are provided with some flexibility in achieving this protection.

GLBA's Safeguards Rule

<16> GLBA's Safeguards Rule uses a "reasonable security" standard.[41] The Safeguards Rule sets forth standards for developing, implementing, and maintaining reasonable security safeguards to protect private consumer information.[42] Businesses trying to comply with A.B. 1950 might find it helpful to look to the Safeguards Rule when they create their security polices and procedures.[43]

<17> The Safeguards Rule requires that businesses develop an information security program that is comprehensive, obtainable in written form, and appropriate to the size, complexity, and the nature of its activities.[44] The security program should be designed to achieve three objectives. It should: (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the customer.[45] In order to achieve these aims, a company's security program should contain provisions for employee training, identifying reasonably foreseeable risks, developing appropriate information systems, and preventing information systems failures.[46]

<18> A business trying to comply with A.B. 1950 should create an information security plan tailored to the business' size and complexity, keeping in mind the three Safeguard Rule objectives. In particular, when borrowing from the Safeguards Rule, a business should be aware of § 314.4. This section defines the elements that a security program should contain in order to meet the three aforementioned objectives. Section 314.4 requires that the security program shall: (1) designate an employee to coordinate the program; (2) identify reasonably foreseeable internal and external risks that might result in an unauthorized disclosure; (3) design and implement information safeguards to control the risks identified in the risk assessment; and (4) oversee service providers to ensure that they are taking appropriate steps to protect private consumer information.[47] These broad requirements allow businesses some flexibility in the implementation. Since complete compliance with GLBA would cause many companies to overspend on information security, businesses should attempt to achieve the Safeguards Rule's objectives by employing only the elements of the Rule that are appropriate and necessary to their business models.

<19> Though the HIPAA Security Rule is far more exhaustive than most businesses need in order to comply with A.B. 1950, it is a useful source from which businesses can borrow standards for three reasons. First, any company complying with HIPAA regulations is exempt from A.B. 1950 because its standards are more exhaustive than A.B. 1950 requires.[48] Second, businesses may rely on HIPAA's Security Rule because it is based on risk management principles that allow businesses to create policies that will meet A.B. 1950's requirements.[49] Finally, the HIPAA Security Rule contains a "flexibility of approach" whereby covered entities can use "any security measures" that allow the covered entity to reasonably implement the required safeguards.[50]

<20> HIPAA's Security Rule is divided into administrative, physical, and technical measures.[51] Administrative measures must contain: (1) fully documented policies and procedures that are used to handle protected health information; (2) security awareness training;[52] and (3) a contingency plan, including policies and procedures, to address emergency situations such as fire, vandalism, or system failure.[53] Next, the required physical measures must consist of three elements: (1) physical access controls;[54] (2) policies about workstation use and security;[55] and (3) device media controls.[56] Finally, technical measures must: (1) encrypt data;[57] (2) guard data integrity though automatic logoffs and other procedures;[58] and (3) generally protect the confidentiality of the data.[59]

<21> In addition to the specific requirements outlined by HIPAA's Security Rule, the Rule also contains general principles that businesses must comply with. In order to comply with HIPAA's Security Rule a covered entity must: (1) ensure confidentiality of information; (2) protect against reasonable anticipated threats or hazards; (3) protect information from misuse within the scope of its reasonably anticipated use; and (4) ensure compliance by its workforce.[60] To achieve compliance, the Security Rule requires businesses to conduct both a risk analysis and risk management assessment.[61] The Security Rule requires the risk analysis to include an assessment of the potential risks and vulnerabilities to confidential information.[62] Risk management, as defined by the Security Rule, is the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable level.[63]

<22> Applying the risk management principles contained in HIPAA allows companies to employ its "flexibility of approach" and choose from the various types of administrative, physical, and technical safeguards that are required under HIPAA. A.B. 1950's "reasonable security procedures" requirement may best be met by companies when they borrow risk management principles from HIPAA.

CONCLUSION

<23> Due to the ambiguous "reasonable security" standard in A.B. 1950, there are no guarantees that businesses complying with GLBA and HIPAA will be immune from liability under A.B. 1950. However, borrowing practices from industries exempted from the law is a common sense approach that should provide businesses with a reasonable degree of protection from liability. Although A.B. 1950 does not explicitly inform businesses how they should employ proper security standards, it does allow businesses to use existing federal standards in order to define security practices and procedures for their unique situations.

PRACTICE POINTERS

- Businesses can remain up to date on the latest California legislation by visiting the website of the California Department of Consumer Affairs Office of Privacy Protection at http://www.privacyprotection.ca.gov/. The website provides overviews of recently enacted and currently pending privacy legislation.
- Stay abreast of the latest developments in the data security arena. For a chronology of data breaches reported since the ChoicePoint incident, see http://www.privacyrights.org.
- When creating a plan to comply with A.B. 1950, businesses should look to the standards developed for compliance with both GLBA's Safeguards Rule and HIPAA's Security Rule. Businesses should consider the following elements in their compliance strategy:

GLBA's Safeguards Rule

- Designate one or more employees to coordinate the safeguards;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select appropriate service providers and contract with them to implement safeguards; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business

arrangements or operations, or the results of testing and monitoring of safeguards. [64]

HIPAA's Security Rule

- Administrative procedures: Create and document business practices to manage the selection and execution of security measures;
- Physical safeguards: Develop a plan for the protection of computer systems and related buildings and equipment from hazards and intrusion; and
- Technical security services: Develop processes that protect and monitor information access and prevent unauthorized access to data that is transmitted over a network.[65]

<< Top

Footnotes

1. Anthony D. Milewski Jr., University of Washington School of Law, Class of 2006. I would like to thank Francoise Gilbert and my editors for their help and patience with this article.
2. A Chronology of Data Breaches Reported Since the ChoicePoint Incident, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 25, 2006).
3. *Identity Theft: What's in a name?*, Economist, May 3, 2005, at 84.
4. Grant Gross, *ChoicePoint to Pay $15 Million for 2005 Data Breach; Data Broker Pays Largest Civil Fine in FTC's History*, PCWorld, Jan. 26, 2006, *available at* http://www.pcworld.com/resource/article/0,aid,124523,pg,1,RSS,RSS,00. . For a detailed account of the ChoicePoint incident, *see* A Chronology of Data Breaches Reported Since the ChoicePoint Incident, http://www.privacyrights.org/ar/CPResponse.htm (last visited Feb. 25, 2006).
5. Gross, *supra* note 4.
6. Various states have also proposed laws to mandate disclosure of security breaches of databases containing personal information. Alaska (H.B. 226, S.B. 148, S.B. 149), Arizona (S.B. 1114), Arkansas (S.B. 1167), California, (S.B. 433, S.B. 852), Colorado (S.B. 137), Georgia (H.B. 638, H.B. 648, S.B. 230, S.B. 245, S.B.

251), Florida (H.B. 129), Illinois (H.B. 1633, H.B. 3743, S.B. 209, S.B. 1479, S.B. 1798, S.B. 1799, S.B. 1899), Indiana (S.B. 503, S.B. 544), Maryland (H.B. 1588/S.B. 1002), Michigan (S.B. 309), Minnesota (H.F. 1410/S.F. 1307, H.F. 1805/S.F. 1805), Missouri (S.B. 506), Montana (H.B. 732), New Jersey (A.B. 1080, A.B. 2048/S.B. 2440), New York (A.B. 1525/S.B. 3141, A.B. 4254/S.B. 2161, A.B. 5487/S.B. 3000, A.B. 6688, A.B. 6903/S.B. 3492, S.B. 2906, S.B. 3494), North Carolina (S.B. 783, S.B. 1048), North Dakota (S.B. 2251), Ohio (H.B. 104, S.B. 89), Oregon (S.B. 626), Pennsylvania (H.B. 1023), Rhode Island (H.B. 5893, S.B. 880), South Carolina (S.B. 669), Tennessee (H.B. 2170/S.B. 2220), Texas (H.B. 1527), Virginia (H.B. 2721), Washington (S.B. 6043), and West Virginia (H.B. 2772) are all considering legislation that would mandate disclosure of personal information upon security breaches, toughen penalties for identity theft, or require that a credit hold be placed on any account holder for whom there may have been a database breach. *See* Mark Rasch, *Cleaning Up Disclosure*, Apr. 11, 2005, http://www.securityfocus.com/columnists/316.

7. Kenneth M. Dreifach, *Data Privacy, Web Security, and Attorney General Enforcement*, 815 PLI/Pat 103, 127 (2004). This incident compromised the personal information of some 265,000 state employees. In addition, the California state controller failed to notify state employees of the attack for two weeks after the breach. *See* John J. Altorelli and Michael K. Lindsey, *New California Law Requires Notification or Security Breaches Involving Personal Information*, 20 No. 10 Computer & Internet L. 10 (2003).

8. Cal. Civ. Code § 1798.82 (West 2005).

9. *Id.* § 1798.83.

10. *Id.* § 1798.81.5.

11. Francoise Gilbert, *Information Privacy and Security in California; The Recent Whirlwind*, 1 No. 2 A.B.A. Sci. & Tech. L. 8, 10 (2004).

12. Lisa J. Sotto and Martin E. Abrams, *Needed: A Master Lock For Data The U.S. Badly Needs A National Standard For Privacy Rules*, Vol. 129, No. 14 The Recorder, Jan. 21, 2005, at 4.

13. *See supra* note 4.

14. Letter from the Nat'l Ass'n of Att'ys Gen., to Linda P. Ford, Sr. V.P. & Legal Couns., CardSystems Solutions, Inc. (June 28, 2005), *available at*

http://www.atg.wa.gov/pubs/SecurityBreach.pdf.

15. Cal. Civ. Code § 1798.82(a) (West 2005). For notification requirements, *see* § 1798.82(g)(1)-(3).

16. *Id.* § 1798.83(a).

17. *Id.* § 1798.81.5(c).

18. John J. Altorelli & Michael K. Lindsey, *New California Law Requires Notification or Security Breaches Involving Personal Information*, 20 No. 10 Computer & Internet L. 10 (2003).

19. Ingrian Networks, *Contending with California Privacy Legislation: Minimizing Exposure to A.B. 1950, S.B. 1 and S.B. 138, available at* http://www.ingrian.com/resources/sol_briefs/cal-leg-sb.pdf.

20. Altorelli, *supra* note 18.

21. Cal. Civ. Code § 1798.83(a) (West 2005).

22. Peter M. Hazelton, Esq. & Dino Tsibouris, Esq., LPA, *April 2005 Privacy and Security Update*, Apr. 2005, *available at* http://www.mt-law.com/Privacy%20and%20Security%20Update%20April%202005.pdf .

23. Saul Ewing, *Technology Transactions and Intellectual Property; Pennsylvania, California Enact New Privacy Laws*, Feb. 2005, *available at* http://www.saul.com/common/publications/pdf_741.pdf.

24. *Id.*

25. Cal. Civ. Code § 1798.81.5(b) (West 2005).

26. *Id.* § 1798.83(e)(6)-(7).

27. *Id.* §§ 1798.81.5(d)(1), 1798.82(e). The combination can be made by either element.

28. *See Id.* § 1798.81.5(d)(2). Medical information is defined broadly. In A.B. 1950 it means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

29. *Id.* §§ 1798.81.5(c)(3), 1798.82(f). For the purposes of these statutes "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

30. *Id.* § 1798.81.5(a) (emphasis added).

31. *Id.* § 1798.81.5(b) (emphasis added).
32. *Id*. § 1798.81.5(c).
33. *Id.* § 1798.81.5(e)(1)-(5).
34. John R. Christiansen, An Integrated Standard of Care For Healthcare and Information Security: Risk Management, HIPAA, and Beyond 106 (2005).
35. *Id*. at 116.
36. Eugene M. Katz & Theodore F. Claypoole, *Willie Sutton is on the Internet: Bank Security Strategy in a Shared Risk Environment,* 5 N.C. Banking Inst. 167, 168-72 (Apr. 2001).
37. Christiansen, *supra* note 33.
38. *Id*.
39. 16 C.F.R. § 314.3(b)(3) (2002).
40. 45 C.F.R. § 164.306(a)(4) (2003).
41. Jon A. Neiditz, *The Other Shoe Drops in Information Security*, November 1, 2004, *available at* http://www.lordbissell.com/Newsstand/Shoe-InformationSecurity-Neiditz-v2.pdf.
42. 16 C.F.R. § 314.1(a) (2002).
43. Lisa J. Sotto et al., New Security Standards for Businesses That Maintain Personal Information (2004), *available at* http://www.hunton.com/files/tbl_s10News/FileUpload44/10865/AB-1950_alert_10.04.pdf.
44. 16 C.F.R. § 314.3(a) (2002).
45. 16 C.F.R. § 314.3(b)(1)-(3) (2002).
46. 16 C.F.R. § 314.4(a)-(e) (2002).
47. *Id*.
48. Cal. Civ. Code § 1798.81.5(e)(1)-(5) (West 2005).
49. 45 C.F.R. § 164.308 (2003).
50. 45 C.F.R. § 164.306(b) (2003).
51. 45 C.F.R. §§ 164.308-.312 (2003).
52. 45 C.F.R. § 164.308(a)(5)(i) (2003).
53. 45 C.F.R. § 164.308(a)(6)-(7) (2003).
54. 45 C.F.R. § 164.310(a)(1)-(2) (2003).

55. 45 C.F.R. § 164.310(b)-(c) (2003).
56. 45 C.F.R. § 164.310(d) (2003).
57. 45 C.F.R. § 164.312(a)(ii)(iv) (2003).
58. 45 C.F.R. § 164.312(a)(ii) (2003).
59. 45 C.F.R. § 164.312 (2003).
60. 45 C.F.R. § 164.306(a)(1)-(4) (2003).
61. 45 C.F.R. § 164.308(a) (2003).
62. 45 C.F.R. § 164.308(a)(1)(ii)(A) (2003).
63. 45 C.F.R. § 164.308(a)(1)(ii)(B) (2003).
64. Fed. Trade Comm'n, Financial Institutions and Customer Data: Complying with the Safeguards Rule (Sept. 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf .
65. D'Arcy Guerin Gue, *The HIPAA Security Rule (NPRM): Overview*, http://www.hipaadvisory.com/regs/securityoverview.htm (Mar. 4, 2006); Practis HIPAA Security Guide, *available at* http://www.epractis.com/HIPAA/security_todolist.htm (last visited Mar. 6, 2006).

<< Top