Washington Journal of Law, Technology & Arts

Volume 4 | Issue 3 Article 5

2-25-2008

Data Privacy and Breach Reporting: Compliance with Various State Laws

G. Martin Bingisser

Constitutional & Regulatory
Cite as: G. Martin Bingisser, *Data Privacy and Breach Reporting: Compliance with Varying State Laws*, 4 Shidler J. L. Com. & Tech. 9 (2/25/2008), *at* <http://www.lctjournal.washington.edu/Vol4/a09Bingisser.html>

DATA PRIVACY AND BREACH REPORTING: COMPLIANCE WITH VARIOUS STATE LAWS

G. Martin Bingisser[1]

Abstract

This Article discusses state laws requiring notification of a party whose personal information is held by a business or government agency when the third party's security is breached and an unauthorized person accesses the personal information. In the wake of the 2005 ChoicePoint data breach, over half of the states passed legislation requiring that companies notify the affected parties after breach of personal information. Most of the state statutes followed the model set forth by California's Security Breach Notification Act of 2002. However, significant variations exist between the different statutes, which can create compliance problems. This Article specifically illustrates the relevant differences, analyzes the effect of the statutes, and discusses the policy implications of such legislation.

Table of Contents

INTRODUCTION

<1>On February 16, 2005 ChoicePoint, a leading supplier of identification and credential verification services, announced that a flaw in their customer screening process had allowed unauthorized users access to the personal information of thousands of people stored on the ChoicePoint servers.[2] ChoicePoint was required to notify the California residents affected by the breach in order to comply with a California law that was passed in the wake of such security breaches. California residents constituted approximately a quarter of the estimated 145,000 individuals affected.[3] The Security Breach Notification Act[4] ("The California Act") was the first legislation requiring that victims of security breaches be notified so that they will be aware of the elevated danger of identity theft and can take steps to protect themselves. While many companies did not publicly disclose security breaches prior to enactment of the California Act, disclosure has been quick under the new law.[5] The success of the California Act and the fear of not having their own citizens

notified has led other states to enact similar legislation.[6]

<2>The Act has brought information security problems into sharper focus. One organization calculated the number of records that have been breached in the United States since January 1, 2005 to be at least 158,937,228.[7] However, these numbers may be overinclusive or underinclusive. Some entities take a maximal compliance approach, and "overnotify," while others may undernotify either to avoid embarrassment or because a breach was not detected.[8] Even the initial estimate of individuals affected by the ChoicePoint breach was conservative because it was based on the number of individuals whose personal information was breached after the California Act went into effect in 2003. As the breaches occurred over a period of time, individuals whose data was breached before that date were not notified.

<3>Because of the increased attention given to security breaches, many other states have adopted similar legislation since the ChoicePoint breach. In March of 2005, Arkansas became the first state to follow California's lead and passed an act modeled on California's statute.[9] As of October 2006, 36 states have passed such legislation,[10] and the trend suggests that more states will be adopting such legislation in the future. Although most of these statutes are modeled after the California Act, some key differences warrant attention because they can create compliance problems for those storing personal information.

THE STRUCTURE OF CALIFORNIA'S ACT

<4>In order to understand the recent legislation requiring notification, one must first understand the California Act that has served as a template for many other statutes.[11] The California Act is one of the broadest in terms of entities covered, applying to all persons, businesses, and state agencies in California that own or license personal information.[12] It requires notification of parties whose personal information is compromised in the event of a breach.[13]

<5>The California Act is also broad in terms of what data is covered. The key terms of the statute are the definition of "security breach," notification requirements, and the definition of "personal information." A security breach is defined as an unauthorized acquisition of data that compromises the security of personal information.[14] Personal information is defined as the first name or initial and last name in combination with either a social security number, driver's license number, other information that would permit access to the individual's financial account (such as a password, PIN number, etc.), or medical information.[15]

<6>The statute mandates that a business, or person conducting business, notify individuals whenever there is a breach exposing those individuals' unencrypted[16] personal information that was, or is reasonably believed to have been, acquired by an unauthorized party.[17] Notification must be sent to all parties reasonably believed to have had their information breached.[18] Notice may be made in writing, electronically, or, when either the costs of notification exceed $250,000 or 500,000 people have been affected, the Act allows for substitute notice, for instance, by notifying major media outlets and posting information about the breach online.[19] Electronic notice is only allowed if it complies with the Electronic Signature Act.[20] Notice must be given "[i]n the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."[21]

VARIATIONS

<7>While nearly every state has used California's model as a basic template, some significant variations exist. States most commonly differ in the breadth of the

statute, the immediacy of notice required, the significance of encryption, and whether or not notice is required when there is not a reasonable threat of harm to the individual.

i. Strict vs. Flexible Statutes

<8>Legislatures have adopted different approaches to the condition that triggers the notification requirement. California requires notification when personal information is acquired.[22] Statues that follow the California Act in this respect are generally stricter in their application, requiring notification even if a breach may not lead to identity theft or financial exposure. In contrast, many states require notification only when the breach of personal information presents a risk of harm to the victims.[23] Such statutes provide companies with more flexible notification requirements.[24] Connecticut is representative of such "flexible" states: its statute does not require notice if it is determined that the breach will "not likely result in harm to the individuals whose personal information has been acquired and accessed."[25] To illustrate, a flexible statute would not require notice after a breach by a "grey hat" hacker,[26] who illegally breaches a system without the intent to commit theft or breach confidentiality. Because such a hacker does not have the intent to do harm, there is no risk of harm to the individuals whose information has been breached, and therefore no notification is required under a flexible statute.

ii. Variations on the Breadth of the Statute

<9>Many states have tailored their statutes to be narrower than the California Act. Georgia, the home of ChoicePoint, narrowed the definition of a breach by applying its Act only to "information brokers."[27] The Georgia statute defines an information broker as a person or entity who engages in the business of "collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals" for the purpose of furnishing such information to third parties.[28] This definition brings a company such as ChoicePoint within the scope of the statute, while a company that collects information for its own use would not be subject to the notification requirements. Georgia and Maine explicitly exclude governmental agencies from their definition of information broker.[29]

<10>Statutes in Illinois and Oklahoma also have a different scope. Illinois applies its statute to all "data collectors."[30] The term includes any entity that handles, collects, or otherwise deals with nonpublic personal information.[31] This definition is quite broad and includes corporations, financial institutions, retail operators, universities, governmental agencies and other similar entities.[32] Oklahoma's statute only applies to state agencies or entities.[33]

iii. Variations on the Definition of Personal Information

<11>California's definition of personal information has been the standard adopted by most states. All states begin by defining personal information as an individual's first name or first initial and his or her last name in combination with a variety of forms of information.[34] The variety of forms of information included in the definition varies from state to state. Nearly every state includes a social security number, driver's license number, or state identification card number in the definition.[35] North Carolina has perhaps the most expansive definition, also including in the definition digital signatures, biometric data, fingerprints, passwords, and the individual's mother's maiden name.[36] Maine and Georgia also include account

passwords in their definition, while North Dakota incorporates digital signatures as well as date of birth and department of transportation photo identification numbers in its definition.[38] Finally, Nebraska and Wisconsin also include mother's maiden name as well as biometric data.[39]

iv. Variations on the Immediacy of Notice Required

<12>Only small variations exist between states concerning the immediacy of notice required. All but one state, Illinois, requires notification in the "most expedient time possible without unreasonable delay."[40] This requirement is conditioned on notification being consistent with the needs of law enforcement agencies and that it occurs after the integrity of the data system has been restored. Illinois, however, has no such condition and requires immediate notification in all circumstances.[41]

v. Variations on the Encryption Requirement

<13>While encryption may not provide a foolproof method of protecting information,[42] the majority of states, like California, do not require notice where a security breach compromises encrypted data unless they lose the key to the encryption.[43] Yet, the statutes typically do not define the type of encryption required to exempt one from the notice requirement.[44] In addition to encryption, several states do not require notification when the identifying information is redacted[45] or if it is otherwise unreadable or unusable.[46]

<14>Three states impose notification requirements even if the data are encrypted. New York and Pennsylvania exempt encrypted data, but require notification if the encryption key has been compromised.[47] North Carolina requires notification for a breach of encrypted information.[48]

vi. Type of Notice Permitted/Required

<15>States vary widely in defining the manner in which notification must be given. Many states disagree over whether and in what manner notice may be given via telephone.[49] The Pennsylvania statute mandates how the offending entity should describe the situation to the harmed individual.[50] The statute also requires that the company provide additional information to an individual in order to aid them in seeking further assistance.[51] Some states also allow for e-mail notification if a prior business relationship exists.[52] Only Maine does not allow for electronic notification.[53] Furthermore, several state statutes require notification of consumer reporting agencies and/or or state authorities.[54]

ANALYSIS

<16>In many respects, the California statute offers the strictest standard of compliance for individuals, companies, and state agencies. California's political influence has allowed states that have not passed such legislation to apply California's legislation to their citizens. At the time of the ChoicePoint breach, California was the only state that had passed such legislation. In the days following ChoicePoint's announcement of the breach, thirty-eight state attorneys general sent letters to ChoicePoint demanding that all affected individuals nationwide be notified using the procedures laid out in California law.[55] Initially, ChoicePoint only sent notification to the 35,000 California residents to whom the statute directly applied. After receiving letters from the state attorneys general, ChoicePoint acquiesced and

notified the remaining affected individuals.[56] However, ChoicePoint's acquiescence seemed to be due to public relations, rather than legal grounds.[57]

<17>A second major incident occurred in the recent AOL search data privacy breach. In August 2006, AOL publicly released search data of more than 650,000 subscribers. [58] Despite a lack of encryption, the breach did not fall within the scope of the various state statutes because the search records were released without any names attached to the records. This meant that the compromised data did not fall within most state's statutory definition of "personal information."[59] Therefore, notification was not required, despite the fact that thorough examination of the search records may reveal the identity of the individuals whose information was breached.[60] AOL has yet to notify the individuals whose data was breached and the company has not yet been required to notify the affected users under the state notification statutes.[61] As this case demonstrates, there are significant holes in the state statutes if they are intended to protect personal information. In effect, most state statutes only protect the individual's financial security. Before notifying individuals, a company should make sure that the breached data falls within the scope of the statutes.

<18>Finally, determining the risk of criminal activity also raises compliance issues in states with flexible statutes. No state statute provides an objective test that can be used to determine if the breach is likely to subject individuals to the risk of criminal activity. An analysis prepared for the Washington State Attorney General has recommended that state attorneys general develop a set of guidelines, but this has not happened.[62] The non-profit organization TrustE encourages companies to develop a similar set of guidelines for internal use.[63] One obvious problem is that trying to quickly determine the intent of hackers may prevent or inhibit an affected company from complying with the timely notification requirements. As such, companies should develop procedures for quickly addressing any breach. By determining what information was breached and by whom, companies may be more able to quickly determine the intent of the hackers and whether notification is required.

POLICY DISCUSSION

<19>The legislative intent of these statutes is to protect the financial security of affected individuals. For example, the North Carolina legislation was entitled the Identity Theft Protection Act.[64] The California Assembly Floor Analyses summarized the legislative intent:

> <20>This bill is intended to help consumers protect their financial security by requiring that state agencies and businesses that keep consumers' personal information in a computerized data system to quickly disclose to consumers any breach of the security of the system, if the information disclosed could be used to commit identity theft. A consumer injured by a violation of the provisions of this bill would have the right to bring civil suit and recover damages.[65]

<21>However, by distinguishing the differences between strict and flexible statutes, the social benefit of flexible statutes is evident. If the goal of a statute is to prevent identity theft and other risks to financial security, then breaches that do not pose any risk to financial security should not be punished. For instance, consider the example used above: if the executive's diskette is found by the well-intentioned stranger, then the notification requirement of a strict statute, such as the California Act, is triggered. This would result in unnecessary money being spent to notify customers. Consumer confidence would also be lowered by evidence of a security breach that has not harmed anyone.

<22>Representative Randall Hultgren of the Illinois Legislature made this exact point when arguing against the bill in a floor debate: "When there's a true breach of security, when there's bad intent out there, we should know about it. But in those accidents…accidental situations or inadvertent situations we don't want to drive banks out of business or lose the confidence of the public in a situation like that."[66]

<23>Few of the states enacting strict statutes have addressed this argument. Even in Illinois, the Legislature passed one of the strictest strict statutes minutes after Representative Hultgren's remarks.[67] The bill was passed against opposition from major interests such as the Illinois Chamber of Commerce and Illinois Bankers Association, which echoed these concerns.[68] The Illinois Act, as discussed above, requires immediate notification even when authorities believe that notification would harm an investigation to track and contain the breach.[69] In fact, a state act could provide a negative social benefit if a company's notification hinders an investigation and leads to further data breaches.

<24>It can also be difficult for companies to determine the existence of a breach in the first place. The most talented hackers may leave little or no trace of their intrusion. Other companies do not have the technology to track intruders. It may be the case that a company only becomes aware that personal information has been compromised when the information is used improperly. In such a scenario, where the damage has already been done, penalizing the company may serve only a limited social benefit. When analyzing strict statutes, Thomas Lenard even concluded that "given these very small expected benefits it is difficult for a notification mandate to pass a benefit-cost test."[70]

<25>Proponents have argued that strict statutes have two advantages over flexible statutes: they deter negligent handling of personal information and are easier to comply with. Notification itself can be harmful to a company's public relations. Therefore, companies might be more diligent in protecting information if they know they will have to notify the public even when no risk is posed. While this may be true, the cost of compliance can be high and other statutes, such as state consumer protection acts,[71] already provide an incentive for companies to protect consumer information.

<26>A better method of preventing identity theft may be to implement preventative measures. For instance, legislatures may want to require companies to outsource the storage of sensitive personal information to companies with more advanced technology. Enacting such strong legislation may be impractical at this time. Congress itself has run into roadblocks in each of its repeated attempts to enact federal legislation concerning this issue. If the real thrust of these statutes is to leverage fair information practices onto businesses, then the social benefits sought may in fact serve the public's interest.[72] Over time, the statute may serve to help the public understand the magnitude of the problem and build support for stronger privacy laws.

CONCLUSION

<27>Companies that store sensitive personal information on their computer systems and suffer security breaches will face complex compliance challenges if they do business in more than one jurisdiction because of differences among state security breach notification laws. While most states follow the model presented in the California Act, many differences exist between jurisdictions. Companies need to be aware of the requirements of each state statue so that they may act accordingly. The differences can be significant; notification may be required in one state while it is not required in another state. While federal legislation could alleviate compliance issues, such an answer will not be found in the near future.

<< Top

Footnotes

1. G. Martin Bingisser, University of Washington School of Law, Class of 2008. The author would like to thank Chris Jay Hoofnagle (University of California, Berkeley School of Law - Samuelson Law, Technology & Public Policy Clinic), Joanne McNabb (California Office of Privacy Protection), and Professor Jane Winn (University of Washington School of Law) for comments on drafts of this article as well as Dan Hadjinian for his editorial assistance.

2. *See* PROTECTING CONSUMER'S DATA: POLICY ISSUES RAISED BY CHOICEPOINT: HEARING BEFORE THE H. SUBCOMM. ON COMMERCE, TRADE, AND CONSUMER PROTECTION, 108th Cong. (2005) (statement of Derek Smith), *available at* http://energycommerce.house.gov/reparchives/108/Hearings/03152005hearing1455/Smith . (Mr. Smith was the Chairman and CEO of ChoicePoint Inc. at the time of the breach).

3. *Id*.

4. CAL. CIV. CODE §§ 1798.80-1798.84 (2007 Supp.).

5. Roy Mark, *Data Brokers Step Into Senate Panel's Fire*, INTERNETNEWS.COM, April 13, 2005, http://www.internetnews.com/ent-news/article.php/3497591.

6. *See* National Conference of State Legislatures, *State Security Breach Notification Laws*, http://www.ncsl.org/programs/lis/cip/priv/breach.htm (last visited March 1, 2007).

7. Privacy Rights Clearinghouse, *A Chronology of Data Breaches Since the ChoicePoint Incident*, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited July 29, 2007).

8. *See* IDENTITY THEFT: INNOVATIVE SOLUTIONS FOR AN EVOLVING PROBLEM: HEARING BEFORE THE S. SUBCOMM. ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY, 110th Cong. (2007) (statement of James Davis), *available at* http://judiciary.senate.gov/pdf/3-21-07DavisTestimony.pdf (discussing the issues faced by organizations when they are required to notify and the reasons behind UCLA's ultimate decision to overnotify following a breach).

9. ARK. CODE ANN. §§ 4-110-101 to -110 (2007 Supp.).

10. ARIZ. REV. STAT. § 44-7501 (2007 Supp.); ARK. CODE ANN. §§ 4-110-101 to -108 (2007 Supp.); CAL. CIV. CODE §§ 1798.80-1798.84 (2007 Supp.); COL. REV. STAT. § 6-1-716 (2007 Supp.); CONN. GEN STAT. § 36a-701b (2007 Supp.); D.C. CODE § 28-3851 (2007 Supp.); DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2005); FLA. STAT. ch. 817.5681 (2006); GA. CODE ANN. §§ 10-1-910 to -912 (2007 Supp.); HAW. REV. STAT. §§ 487N-1 to -4 (2007 Supp.); IDAHO CODE ANN. §§ 28-51-104 to -107 (2007 Supp.); 815 ILL. COMP. STAT. 530/1 to /30 (2007 Supp.); IND. CODE §§ 24-4.9-1-1 to -3-4 (2006); KANSAS STAT. §§ 50-7a01 to -7a04 (200 Supp.); MD. CODE ANN., COM. LAW § 14-3501 to -3508 (2007 Supp.); ME. REV. STAT. ANN. tit. 10, §§ 1346 to 1350-A (2007 Supp.); MICH. COMP. LAWS § 445.71 (2007 Supp.); MINN. STAT. § 325E.61 (2007 Supp.); MONT. CODE ANN. § 30-14-1704 (2007); NEB. REV. STAT. § 87-801 to -807 (2007); NEV. REV. STAT. § 603A.220 (2007 Supp.); N.H. REV. STAT. ANN. §§ 359-C:19 to :21 (2007 Supp.); N.J. STAT. ANN. § 56:8-163 (2007 Supp.); N.Y. GEN. BUS. LAW §

899-aa (2008 Supp.); N.C. GEN. STAT. § 75-65 (2007); N.D. CENT. CODE §§ 51-30-01 to -07 (2007); OHIO REV. CODE ANN. § 1349.19 (2005); 74 OKLA. STAT. § 3113.1 (2008 Supp.); 2007 OR. LAWS 759; 73 PA. CONS. STAT. §§ 2302-2303 (2007 Supp.); R.I. GEN LAWS § 11-49.2-1 to -7 (2006 Supp.); TENN. CODE ANN. § 47-18-2107 (2007 Supp.); TEX. BUS & COM. CODE ANN. § 48.103 (2007 Supp.); UTAH CODE ANN. § 13-44-101 (2007 Supp.); VT. STAT. ANN. tit. 9, § 2430 to -2435 (2006); WASH. REV. CODE § 19.255.010 (2006); WIS. STAT. § 895.507 (2006). *See also* Perkins Coie, *Security Breach Notification Chart*, http://www.perkinscoie.com/statebreachchart/ (last visited Jan. 8, 2008).

11. *E.g.*, H.B. 1633 Transcripts of Debate, 94th Gen. Assembly (Ill. 2005) (statement by Representative John Fritchey that "Some had said, let's just take what California had done and roll that out. We went beyond that, we've scaled back.").

12. CAL. CIV. CODE §§ 1798.82.

13. *Id.*

14. CAL. CIV. CODE § 1798.82(d).

15. CAL. CIV. CODE § 1798.82(e).

16. The California Act, as well as the legislation in most other state, does not define the words 'encryption,' 'encrypted,' or 'unencrypted.' North Carolina is one of the few states to define encryption: "The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." N.C. GEN. STAT. § 75-61(8). Arkansas' definition of encryption is broader than the common usage of the term:

    > "Encryption," as used here means "the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to (i) prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; (ii) cause or make any data, information, image, program, signal or sound unintelligible or unusable; or (iii) prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.

    ARK. CODE ANN. §§ 4-110-101 to -110.

17. CAL. CIV. CODE § 1798.82(a).

18. *Id.*

19. CAL. CIV. CODE § 1798.82(g). Substitute notice is given by performing all of the following: e-mail to the person or business affected, conspicuous posting on the company web page, notification to statewide media. Cal. CIV. CODE § 1798.82(g)(3).

20. CAL. CIV. CODE § 1798.82(g)(2).

21. CAL. CIV. CODE § 1798.82(a).

22. *Id.*

23. *See, e.g.*, CONN. GEN. STAT. § 36a-701b.

24. The State Public Interest Research Groups (PIRG) refers to the two types of statutes respectively as Exposure and Risk statutes. State

Public Interest Research Groups, *Summary of State Security Freeze and Security Breach Notification Laws*, http://www.pirg.org/consumer/credit/statelaws.htm (last visited January 21, 2007).

25. Conn. Gen. Stat. § 36a-701b. The language used in Washington's flexible statute also creates a problem. Wash. Rev. Code § 19.255.010. The statute requires notification if the "customer" is subjected to a risk of criminal activity. While the term "resident of the State" is used elsewhere in the statute, "customer" is used in this sentence. This creates an issue because in many breaches, it is not the customer's personal information that is breached. For instance, none of the individuals whose personal information was breached in the ChoicePoint case were "customers" of ChoicePoint.

26. Hackers are generally divided into three groups. "Black hat" hackers typically hack for personal gain or to inflict damage. "White hat" hackers typically hack into their own systems or those of a client in order to test security. "Grey hat" hackers typically possess the intent of "white hat" hackers, but do not have authority to hack into the system. Red Hat, Inc., *Red Hat Linux Security Guide* § 2.1.1 (2002), http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/pdf/rhl-sg-en-9.pdf.

27. Ga. Code Ann. § 10-1-912(a).

28. Ga. Code Ann. § 10-1-911(2).

29. *Id.*; Me. Rev. Stat. Ann. tit. 10, §§ 1346 to 1350-A.

30. 815 Ill. Comp. Stat. 530/1 *et seq.*; Ind. Code § 24-4.9; 74 Okla. Stat. § 3113.1.

31. *See, e.g.*, 815 Ill. Comp. Stat. 530/5.

32. *Id.*

33. 74 Okla. Stat. § 3113.1.

34. *See, e.g.*, Cal. Civ. Code § 1798.82(e).

35. *See, e.g.*, *id.*

36. N.C. Gen. Stat. § 75-61(10).

37. Me. Rev. Stat. Ann. tit. 10, § 1347(6); Ga. Code Ann. §§ 10-1-911(6).

38. N.D. Cent. Code § 51-30-01(2)(a).

39. Neb. Rev. Stat. § 87-802(5); Wis. Stat. § 895.507(b).

40. *See, e.g.*, Cal. Civ. Code § 1798.82(a).

41. The Illinois statute was modeled after the California Act. It was not until the final house amendment that the language was changed to require notification immediately following discovery, despite what authorities may deem. The Legislative history does not illustrate why this change was made. H.B. 1633 House Amendment No. 4, 94th Gen. Assembly (Ill. 2005).

42. *See* Niels Ferguson and Bruce Schneier, Practical Cryptography 7 (2003):

> Too many engineers consider cryptography to be a sort of magic security dust that they can sprinkle over their hardware or software, and which will imbue those products

with the mythical property of "security" … Security is only as strong as the weakest link … it's the things around the cryptography that make the cryptography effective.

43. *See, e.g.*, WASH. REV. CODE 19.255.010(1).

44. *See, e.g.*, CAL. CIV. CODE § 1798.82(e).

45. Arizona, Arkansas, Colorado, Illinois, Indiana, Kansas, Louisiana, Maine, Nebraska, Pennsylvania, and Vermont do not require notification when redacted information has been compromised.

46. Arizona, Colorado, Connecticut, Nebraska, Ohio, Vermont, and Wisconsin do not require notification if the information is otherwise unreadable or unusable.

47. N.Y. GEN. BUS. LAW § 899-aa; 73 PA. CONS. STAT. § 2303. An encryption key is a sequence of characters that deciphers the encryption code.

48. N.C. GEN. STAT. § 75-65(a).

49. Colorado, Utah, Arizona, Connecticut, Hawaii, Idaho, Montana, Nebraska, North Carolina, Ohio, Pennsylvania, and Rhode Island have all adopted different requirements than California in regards to telephone notification.

50. 73 PA. CONST. STAT. § 2302.

51. *Id.*

52. *Id.*

53. ME. REV. STAT. ANN. tit. 10, §§ 1346 *et seq*.

54. *See, e.g.*, ME. REV. STAT. ANN. tit. 10, § 1348 (requiring notification of both consumer reporting agencies and state regulators).

55. The Associated Press, *38 AGs Send Open Letter To ChoicePoint*, USA TODAY, Feb. 19, 2005, *available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-19-ag-letter-to-choicepoint_x.htm.

56. Smith, *supra* note 2.

57. However, it has been advocated by the Agora that Washington State should adopt language requiring all individuals to be notified in the event of a breach. Current statutes only require that residents of the state be notified. *See* The Agora, *SB 6043 - Washington State's New Disclosure Law: Comments and Guidance* (Sept. 2005) (unpublished manuscript, on file with the Shidler Journal of Law, Commerce & Technology).

58. *AOL Tells of Breach of Privacy*, LOS ANGELES TIMES, Aug. 8, 2006, at C6.

59. CAL. CIV. CODE § 1798.82(e) defines "personal information" as "an individual's first name or first initial and last name in combination with any one or more of the following data elements…" As no names were included in the released search data, the notification statutes were not triggered.

60. A New York Times article used publicly available data, combined with the released search data, to successfully identify a user. Michael Barbaro and Tom Zeller, *A Face is Exposed for AOL Searcher No. 4417749*, NEW YORK TIMES, Aug. 9, 2006, *available at*

http://www.nytimes.com/2006/08/09/technology/09aol.html?hp&ex=1155182400&en=9b5fd9ff341e3216&ei=5094&partner=homepage .

61. Apparently, the only action taken against AOL so far has been a lawsuit by three customers alleging violation of the Federal Electronic Communications Privacy Act as well as California consumer protection laws. *AOL is Sued Over Privacy Breach*, Los Angeles Times, Sept. 26, 2006, at C2. The Federal Trade Commission has also filed a complaint against AOL for, among other things, breaching their own privacy policy. *See In the Matter of AOL LLC, a majority-owned subsidiary of Time Warner Inc.*, August 14, 2006, *available at* http://www.eff.org/Privacy/AOL/aol_ftc_complaint_final.pdf.

62. *See* The Agora, *SB 6043 - Washington State's New Disclosure Law: Comments and Guidance* (Sept. 2005) (unpublished manuscript, on file with the Shidler Journal of Law, Commerce & Technology).

63. TrustE, *Security Guidelines 2.0*, http://www.truste.org/pdf/SecurityGuidelines.pdf (last visited Jan. 21, 2007).

64. N.C. Gen. Stat. § 75-60.

65. California State Assembly, *Bill Analysis of S.B. 1386*, Aug. 8, 2002, *available at* http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_20020823_220958_asm_floor.html.

66. H.B. 1633 Transcripts of Debate, 94th Gen. Assembly (Ill. 2005).

67. *Id.*

68. *Id.*

69. 815 Ill. Comp. Stat. 530/1 to /30.

70. Thomas Lenard and Paul Rubin, *An Economic Analysis of Notification Requirements for Data Security Breaches*, Progress on Point 12.12, July 2005, at 12, http://www.pff.org/issues-pubs/pops/pop12.12datasecurity.pdf. This research is underscored by reports by Visa stating that only two percent of compromised credit card numbers are used fraudulently.

71. *See, e.g.*, Wash. Rev. Code § 19.86.020.

72. Deirdre Mulligan and Chris Jay Hoofnagle made this point before a Senate Subcommittee while noting that the statutes create an incentive for investment in best information security practices. *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the S. Subcomm. On Terrorism, Technology, and Homeland Security*, 110th Cong. (2007) (statement of Deirdre K. Mulligan and Chris Jay Hoofnagle), *available at* http://judiciary.senate.gov/pdf/3-21-07HoofnagleTestimony.pdf.