Security Breach Notifications: State Laws, Federal Proposals, and Recommendations

MILTON C. SUTTON*

ABSTRACT

Many firms are in the business of storing vast sums of consumer information. The fields of data include but are not limited to: name, address, date of birth, driver's license number, social security number, financial account number, as well as credit card number. In the past, there were instances where consumer data was breached by computer hackers or stolen through employee neglect or dishonesty. However, these thefts were relatively small and did not make major news. This changed in 2005, when the firm ChoicePoint began an incident disclosure and notification process of a security breach that compromised the personal information of over 145,000 people. This article will address: (1) recent news involving substantial security breaches and an overview of the problem, (2) observations from the recent waive of breaches, (3) responses to security breaches at the state level, (4) proposed responses to security breaches at the federal level, (5) actions of the international community to curb security breaches, and (6) policy recommendations.

I. INTRODUCTION

There have been over a dozen major security breaches at various brokers, universities, banks, and other institutions which have led to the exposure and potential identity theft of millions of consumer records. On February 15, 2005, ChoicePoint, a corporation that collects and compiles information that includes personal and financial information on millions of consumers, disclosed that it had begun a notification process due to a security breach, which compromised the personal data of approximately 145,000 people.[1] Criminals gained access to the personal data by posing as small businesses.[2] ChoicePoint was the starting point of a string of public disclosures concerning data breaches in 2005.[3]

---

* Milton Sutton is a juris doctor candidate at The Ohio State University Moritz College of Law, class of 2007. He holds a bachelor's degree in business: computer information systems from Indiana University.

[1] Michael Rasmussen, *ChoicePoint Security Breach Will Lead To Increased Regulation*, FORRESTER, Mar. 3, 2005, http://www.csoonline.com/analyst/report3416.html.

[2] *Id.*

[3] *Id.*

On February 25, Bank of America disclosed that it had lost a backup tape which contained personal information of over 1.2 million customers in what may be the biggest security breach to date within the banking industry.[4] In one incident, an employee was in the process of transporting a digital tape that contained private consumer information while on a commercial airline flight when it was lost.[5] The tapes contained credit card account records of federal employees, including sixty U.S. senators.[6] In another incident, an individual fraudulently posed as a collection agency and purchased account information on customers from a bank employee.[7]

On March 10, LexisNexis had its passwords compromised which led to the theft of over 32,000 customer records.[8] According to Kurt P. Sanford, head of LexisNexis corporate and federal markets group, "perpetrators used computer programs to generate IDs and passwords that matched those of legitimate customers. In other cases . . . hackers appear to have collected IDs and passwords after using computer viruses to collect the information from infected machines as they were being used."[9] Similar to the ChoicePoint breach, "unauthorized parties also set up accounts with LexisNexis posing as legitimate businesses."[10]

In June, CardSystems revealed that it had a security breach in which "information on more then 40 million credit cards may have been stolen."[11] This could be the largest security breach on record.[12]

---

[4] *See* Grant Gross, *Senators Rip into ChoicePoint, Bank of America*, SECURITY.ITWORLD.COM, Mar. 11, 2005, http://security.itworld.com/5010/050311senatorsrip/page_1.html.

[5] *Id.*

[6] *Id.*

[7] *Bank Security Breach May be Biggest Yet*, CNNMONEY.COM, May 23, 2005, http://money.cnn.com/2005/05/23/news/fortune500/bank_info/.

[8] *See* Gross, *supra* note 4.

[9] Jonathan Krim, *LexisNexis Data Breach Bigger Than Estimated*, WASH. POST, Apr. 13, 2005, at E01, *available at* http://www.washingtonpost.com/wp-dyn/articles/A45756-2005Apr12.html.

[10] *Id.*

[11] Joris Evers, *Credit Card Breach Exposes 40 Million Accounts*, CNET NEWS.COM, June 17, 2005, http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html.

"CardSystems is one of several companies that process transactions for banks and merchants."[13] The breach was made possible by use of security vulnerabilities in the company's network which allowed the intruder to access cardholder data.[14]

II. OBSERVATIONS

Security breaches have affected approximately 50 million people, according to the Privacy Rights Clearinghouse.[15] "While there have been major security breaches at commercial data brokers such as LexisNexis . . . there have also been security problems at banks, schools, government entities such as motor vehicle administrations, and retailers. This demonstrates the need for intervention across a broad array of entities."[16]

Beyond committing identity theft, there are other reasons that security breaches occur. For instance, "insiders at Bank of America, Wachovia, PNC Bank and Commerce Bank sold customers' personal information to attorneys and others who were engaged in debt collection efforts."[17] Systems have been known to be compromised for voyeuristic purposes. The goal is to obtain the "contact information or communications data of celebrities or law enforcement officials."[18] Breaches have also been motivated by competitive

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Data Security: The Discussion Draft of Data Protection Legislation: Hearing on the Discussion Draft of Data Protection Legislation Before the H. Comm. on Energy and Commerce*, 109th Cong. (2005) (statement of Chris Jay Hoofnagle Director and Senior Counsel, Electronic Privacy Information Center West Coast Office), *available at* http://www.epic.org/privacy/choicepoint/datasec7.28.05.html.

[16] *Id.*

[17] *Data Security: The Discussion Draft of Data Protection Legislation*, *supra* note 15 (quoting Jonathan Krim, *Banks Alert Customers of Data Theft*, WASH. POST, May 26, 2005, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/05/25/AR2005052501777.html).

[18] *Id.* (quoting Kelly Martin, *Hacker Breaches T-Mobile Systems, Reads US Secret Service Email and Downloads Candid Shots of Celebrities*, SECURITYFOCUS, Jan. 12, 2005).

reasons such as obtaining vital information about a competitor.[19] Extortion is another motivation to obtain information with the threat of disclosure.[20] The events in 2005 demonstrate that a major source of the security problem originates from corrupt or dishonest employees.[21] Currently, a national standard does not exist detailing how firms should properly deal with issues regarding security breaches. According to Andreas M. Antonopoulos,

> a little-noticed provision of the Fair and Accurate Credit Transactions Act (often referred to as the "FACT Act," or "FACTA"), which amended the Fair Credit Reporting Act ("FCRA") adds an interesting twist to the identity-theft issue. In the amended act, financial institutions are required to identify 'red flags' that may indicate identity theft. This applies not only to the major credit clearing houses, but also to any financial agency that stores and uses credit reports. Furthermore, under the act, financial institutions that provide information to credit bureaus must ensure the accuracy and integrity of that information.[22]

To meet the Gramm-Leach-Bliley Act, agencies have adopted a further clarification of breach notifications published by the Office of Comptroller of Currency, Board of Governors of the Federal Reserve, Office of Thrift Supervision, and the Federal Deposit Insurance Corporation.[23]

With the guidelines proposed, according to Mr. Antonopoulos, "there is a new requirement for breach notification that, through the Gramm-Leach-Bliley Act, is a national standard for all financial services institutions. The guideline reads: '[t]he institution should, under certain circumstances, notify affected customers when sensitive

---

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Andreas M. Antonopoulos, *Are California's Database Breach Notification Rules Going National?*, NETWORK WORLD, Apr. 4, 2005, http://www.networkworld.com/newsletters/datacenter/2005/0425datacenter1.html.

[23] *See id.*

customer information about them is the subject of unauthorized access.'"[24]

III. RESPONSES AT THE STATE LEVEL

As stated above, in early 2005, ChoicePoint revealed that a security breach had occurred upon which it sold the personal information of almost 145,000 people to criminals. "The company first disclosed the breach only to California residents, as required by California's 'Notice of Security Breach' law, enacted in 2002. However, the company later disclosed that residents in other states, the District of Columbia and three territories also may have been affected by the ChoicePoint breach."[25] Since these disclosures, additional states have introduced legislation requiring that companies and/or state agencies disclose to consumers security breaches involving personal information.

A. CALIFORNIA

California is the first state to pass measures requiring disclosure by firms that collect personal information when there is a breach. California Senate Bill 1386 requires California agencies, persons, or business who collect personal data to disclose any breach of security involving such data to residents of the state who's information is "reasonably believed" to have been obtained by an unauthorized individual.[26]

"The California law requires that firms notify customers about their breached personal information in the 'most expedient time possible' and 'without unreasonable delay.'"[27] The law "allows firms to delay notification if a law enforcement agency determines that the

---

[24] *Id.*

[25] National Conference of State Legislatures, 2005 Security Breach Notification/Legislation, http://www.ncsl.org/programs/lis/cip/priv/breach05.htm (last visited Nov. 28, 2005).

[26] *See* S.B. 1386 Senate Bill – CHAPTERED (Sept. 26, 2002), http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

[27] *See* Gibson, Dunn & Crutcher LLP, *Security Breach Notifications: A State and Federal Law Maze*, July 27, 2005, http://www.gibsondunn.com/practices/publications/detail/id/766/?pubItemId=7832.

notification will impede a criminal investigation."[28] Notice is usually required in written or electronic form.[29] California "allows a firm to bypass these procedures if the firm complies with its own notification procedure and is 'otherwise consistent' with the law's timing requirements."[30] The law also "places a duty on firms that only maintain computerized data but do not own that data to notify the owner or licensees of the information in case of a security breach."[31] Finally, the law "creates a civil cause of action against firms that do not notify California resident after a security breach. An action could also be brought under California's Business and Professions Code Section 17200, including for attorneys' fees."[32]

B. DELAWARE

Delaware passed House Bill 116 in June of 2005. The bill's purpose is to assist in assuring that personal information about Delaware residents is protected.[33] The bill "encourages data brokers to provide reasonable security for personal information."[34] Specifically, it requires the following.

> [1] an individual or a commercial entity that conducts business in Delaware and [2] that owns or licenses computerized data that includes personal information [3] to notify a resident of Delaware of any breach of the security of the system immediately following the discovery of a breach in the security of personal information of the Delaware resident [4] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification must be made in good

---

[28] *Id.*

[29] *Id. See also* Cal. Civ. Code § 1798.82(g).

[30] *Id. See also* Cal. Civ. Code § 1798.82(h).

[31] *Id. See also* Cal. Civ. Code § 1798.82(b).

[32] *Id. See also* Cal. Civ. Code §§ 1798.82, 1798.84.

[33] National Conference of State Legislatures, *supra* note 25.

[34] *Id. See also* H.B. 116, 143rd Gen. Assem., Reg. Sess. (Del. 2005).

> faith, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.[35]

C. NEW YORK

New York passed Senate Bill 3492 signed in August of 2005. The legislation "[r]equires any state agency or businesses [owning or licensing] a computerized database" with personal information to "disclose any breach of security of [that] system to any resident of New York . . . whose unencrypted data may have been acquired by an unauthorized person."[36]

D. NEW JERSEY

New Jersey passed the "Identity Theft Prevention Act" in September 2005.[37] The bill "requires any firm that conducts business in New Jersey or any public entity that compiles or maintains computerized records that include personal information to disclose any breach of security to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[38]

Governmental agencies and businesses who maintain and store records for other business or public entities must notify that business or public entity if there is a breach.[39] The business or public entity then "shall notify its New Jersey customers of the breach."[40] However, if the agency or business proves that the information is such

---

[35] *Id.*

[36] *Id. See also* A.B. 4254/S.B. 3492, 2005 Assem., Reg. Sess. (N.Y. 2005).

[37] Identity Theft Prevention Act, Assem. Comm. Substitution for A.B. 4001/S.B. 2665, 211th Leg., Reg. Sess. (N.J. 2005).

[38] National Conference of State Legislatures, *supra* note 25.

[39] *Id.*

[40] *Id.*

that it cannot be misused, disclosure is not required.[41] These types of determinations are to be documented and kept for five years.[42]

Furthermore, if a law enforcement agency believes that such notification will hamper a criminal investigation, disclosure may be delayed.[43] Such notice can come in electronic or written form.[44]

> [I]f the business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds $500,000, or the business does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major statewide media. However, a business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system.[45]

Moreover, businesses must take all reasonable steps to ensure personal customer data that is no longer needed is destroyed. This can be done by shredding, erasing, or any modification to ensure the data is unreadable or undecipherable.[46]

It is apparent that most states followed California's notification law when drafting their own legislation. Legislation was introduced in

---

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] National Conference of State Legislatures, *supra* note 25.

[45] *Id.*

[46] *Id.*

at least thirty-five states by June 2005,[47] and as of October 27, 2005, at least twenty-two states have enacted laws in the area of security breach notifications.[48]

IV. PROPOSED RESPONSES AT THE FEDERAL LEVEL

The wave of public disclosures over the past year has prompted elected officials at the federal level to respond. Various federal legislators have drafted legislation to address security breaches in an effort to establish a national standard for proper disclosure and penalties.[49]

A. SENATOR SPECTER OF PENNSYLVANIA

Senator Arlen Specter has proposed the Personal Data Privacy and Security Act of 2005 (S. 1789) which would amend the federal criminal code to prohibit: (1) intentionally accessing a computer without authorization, thereby obtaining data broker information; (2) concealing security breaches involving personally identifiable information (personal information); and (3) unlawfully accessing

---

[47] *Id.* (Those states which have legislation pending include: Alaska, Arizona, Maryland, Massachusetts, Michigan, Missouri, Oregon, South Carolina, Virginia, West Virginia, and Wisconsin).

[48] *Id.* (Those states which have enacted laws include Arkansas *(S.B. 1167)*, Connecticut *(S.B. 650)*, Delaware *(H.B. 116)*, Florida *(H.B. 481)*, Georgia *(S.B. 230)*, Illinois *(H.B. 1633* and *S.B. 1799)*, Indiana *(S.B. 49* and *S.B. 503)*, Louisiana *(S.B. 205)*, Maine *(L.D. 1671)*, Minnesota *(H.F. 225/S.F. 361* and *H.F. 2121/S.F. 2118)*, Montana *(H.B. 732)*, Nevada *(A.B. 334, A.B. 1,* and *S.B. 347)*, New Jersey *(Assembly Committee Substitute for A.B. 4001 / S.B. 2665 / Senate Committee Substitute for Senate Bill Nos. 1914, 2154, 2155, 2440, 2441 and 2524 / A.B. 2048)*, New York *(A.B. 4254/S.B. 3492* and *A.B. 8397/S.B. 5827)*, North Carolina *(H.B. 1248 / S.B. 1048)*, North Dakota *(S.B. 2251)*, Ohio *(H.B. 104)*, Pennsylvania *(S.B. 712)*, Rhode Island *(H.B. 6191)*, Tennessee (H.B. 2170 / S.B. 2220), Texas *(S.B. 122)* and Washington *(S.B. 6043)*).

[49] There are currently four bills in the House of Representatives and three in the Senate. Those include H.R. 3140 (Rep. Melissa Bean [IL – 8]), H.R. 3501 (Rep. Julia Carson [IN – 7]), H.R. 4127 (Rep. Cliff Stearns [FL – 6]), H.R. 3374 (Rep. Steve LaTourette [OH – 14]), S. 1597 (Sen. Jon Corzine [NJ]), S. 1326 (Sen. Jeff Sessions [AL]), and S. 1408 (Sen. Gordon Smith [OR]).

another's means of identification during a felony involving computers.[50]

It amends the Racketeer Influenced and Corrupt Organizations Act[51] to cover fraud in connection with such unauthorized access and directs the U.S. Sentencing Commission to amend the sentencing guidelines regarding identity theft.[52] The bill, at ninety-one pages (compared to Senator Feinstein's which is less than ten), is the most far reaching and detailed of any of the legislation proposed to date. It includes a provision which would make notice to law enforcement (specifically, the Secret Service) after a breach mandatory when the breach involves more than 10,000 individuals nationwide. It provides for enhanced punishment for fraud and similar criminal acts connected with accessing personal information without authorization, organized crime involving data and its unauthorized access, and cover ups of such breaches.[53]

The proposed Act would also grant assistance for state and local law enforcement agencies in order to combat crimes related to criminal use of personal identifiable information.[54] Businesses would be exempt only if they completed a risk assessment, which would have to be conducted with federal law enforcement and the state attorney general.[55] This risk assessment would involve individual businesses utilizing security programs and policies which provide notice after a breach.[56]

The Act would also provide victim protection assistance, which would require the business or agency to provide the consumer with

---

[50] *See* S. 1332, 109th Cong. (1st Sess. 2005) (related to S. 1789), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1332pcs.txt.pdf.

[51] Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961-1968 (2006).

[52] *Id.* at §§ 102 and 105.

[53] S. 1332, 109th Cong. §§ 101-103 (1st Sess. 2005), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1332pcs.txt.pdf.

[54] *Id.*

[55] *Id.*

[56] *Id.*

monthly access to credit reports and credit monitoring services for up to one year from the date of a notice of a breach to that consumer.[57] The Act would set a national standard for the protection of social security numbers; more specifically, it would make it illegal for any person to display an individual's social security number to a third party without voluntary or express consent.[58] The Act also makes it illegal to sell or purchase any social security number of an individual without voluntary or express consent.[59] Finally, the bill would require studies in order to establish a consensus of best practices, policy standards and solutions.[60]

B. SENATOR FEINSTEIN OF CALIFORNIA

Senator Dianne Feinstein has proposed the Notification of Risk to Personal Data Act (S. 751).[61] The bill is based largely on the legislation passed at the state level in California with some modifications. The Act requires:

> any agency or person . . . that owns or licenses electronic data containing personal information . . . following the discovery of a breach of security of the system containing such data, [to] notify any resident of the United States whose . . . personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[62]

It requires any agency or person who possesses, but does not own or license such data, to notify the information owner or licensee about such an unauthorized acquisition.[63] There is an allowance of a delay

---

[57] *Id.*

[58] *Id.*

[59] S. 1332, 109th Cong., *supra* note 53.

[60] *Id.*

[61] S. 751, 109th Cong. (1st Sess. 2005).

[62] S. 115, 109th Cong. (1st Sess. 2005) (related to S. 751), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s115is.txt.pdf.

[63] *Id.*

of notification in connection with authorized law enforcement purposes and provides authorized methods of notification and alternative notification procedures.[64] Notice may be written or electronic.[65] If the business demonstrates that "the cost of providing notice would exceed $250,000 [or that] the affected class of subject persons to be notified exceeds 500,000; or the [business] does not have sufficient contact information for those to be notified," it may provide substitute notice.[66]

Finally, the proposed act contains stronger provisions than its California counterpart. The act "covers both electronic and nonelectronic data, includes encrypted as well as non-encrypted data, closes the 'loophole' that allows companies to follow weaker notification requirements, lays out specific requirements for what must be included in notices, and it has tougher penalties."[67]

1. CRITIQUE AND RECOMMENDATIONS ON THE PROPOSED LEGISLATION

Both the Personal Data Privacy and Security Act of 2005 and the Notification of Risk to Personal Data Act are a great start to address the crisis of security breach notifications and identity theft that have become, unfortunately, common since 2004 and through 2005.

Senator Specter's bill is an excellent proposal and begins to address the issues surrounding security breaches. The bill, however, needs an easy-to-read format that would make the disclosure of organizations' privacy statements and notification policies mandatory, and in an easy-to-read format. A good privacy statement should be concise and provide adequate notice of the organization's privacy policies to all persons whose information is sought.[68] The bill should also include a section for organizations whose main business involves customer finances, such as banks, to include mandatory monitoring programs that are capable of "detect[ing] actual and attempted attacks

---

[64] *Id.*

[65] *Id.*

[66] *Id.* at § 3.

[67] *See* Rodney Petersen, *Security Breaches: Notification, Treatment, and Prevention*, 40 EDUCAUSE REV. 78, July/Aug. 2005, *available at* http://www.educause.edu/apps/er/erm05/erm05413.asp?bhcp=1.

[68] *Id.*

on customer information systems."[69] Such systems are essential in preserving trust in consumer information systems as well as to implement an effective response program.[70] Finally, the bill should require high-level officers to be held more accountable by having certification requirements in place in regard to the accuracy of the notification disclosures.[71]

Senator Feinstein's Notification of Risk to Personal Data Act,[72] while far reaching, does not go quite far enough. There are no protections for persons who are victims of identity theft. Senator Feinstein's bill should also include victim protection assistance to protect the credit histories of consumers. Either bill, if passed would provide consumers with greater confidence that their information is being protected and that those who seek to commit crimes by maliciously stealing their information will be strongly pursued under the law.

There is potentially a concern, however, that consumers may become overly accustomed to notifications and, therefore, not take them seriously. This possible effect highlights the importance of balancing the requirements of business (prevention of security breaches) with the needs of the consumer (protection of personal information). As a result, there is a vital need for a national policy.

V. ACTIONS OF THE INTERNATIONAL COMMUNITY

More than a decade ago, the European Union ("EU") took steps similar to what is currently being proposed in the United States Congress. In October 1995, the European Union passed Directive 95/46/EC on the protection of personal data.[73] It created a framework with the goal of striking a balance between protection for the privacy of individuals and the free movement of personal data. The Directive

---

[69] Comments of the Electronic Privacy Information Center on Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Oct. 14, 2003), http://www.epic.org/privacy/glba/noticecomments.html.

[70] *Id.*

[71] *Id.*

[72] S. 751, 109th Cong. (1st Sess. 2005).

[73] Council Directive 95/46; 1995 O.J. (L 281) (EC); SCADPlus: Protection of Personal Data, http://europa.eu.int/scadplus/leg/en/lvb/l14012.htm (last visited Mar. 6, 2006).

puts in place restrictions on the collection and use of personal data, and each Member State must create an independent national body to implement these policies.[74]

The Directive "applies to data processed by automated means (e.g., a computer database of customers) and data contained in or intended to be part of non automated filing systems (traditional paper files)."[75] The Directive provides that all persons have a right to access their data. The guidelines specify that processing of personal data must be done through fair and lawful means and collected for specific and legitimate functions.[76] Data is required to be accurate and up to date; moreover,

> personal data may be processed only if the data subject has unambiguously given his/her consent or processing is necessary:
>
> - for the performance of a contract to which the data subject is party or;
> - for compliance with a legal obligation to which the controller is subject or;
> - in order to protect the vital interests of the data subject or;
> - for the performance of a task carried out in the public interest or;
> - for the purposes of the legitimate interests pursued by the controller.[77]

Exemptions and restrictions exist "in order to safeguard aspects such as national security, defense, public security, [and] the

---

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

prosecution of criminal offences," and for "an important economic or financial interest of a Member State or of the European Union or the protection of the data subject."[78] Individuals have the right to object to their information being collected, and the Directive also sets forth standards to protect confidentiality and security of processing. The Directive stipulates the following.

> [A]ny person acting under the authority of the controller, [the person who collects personal data,] or of the processor, [the person who works with such data,] . . . must not process [the data] except on instructions from the controller. In addition, the controller must implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.[79]

The Directive also deals with the issue of notification. The Directive calls upon a national supervisory authority to oversee policies laid down by those who collect personal data.

> [T]he controller must notify the national supervisory authority before carrying out any processing operation. Prior checks to determine specific risks to the rights and freedoms of data subjects are to be carried out by the supervisory authority following receipt of the notification. Measures are to be taken to ensure that processing operations are publicized and the supervisory authorities must keep a register of the processing operations notified.[80]

The Directive does not require notice upon a security breach.

VI. CONCLUSION

With the sustained and continued disclosures of security breaches that have occurred over the past year, states have taken the initiative to

---

[78] *Id.*

[79] Counsel Directive 95-46, *supra* note 73.

[80] *Id.*

pass laws which address proper notification for the breach of their citizens' private information. Because many of the firms that have been the victim of breaches are large, the number of victims can reach into the millions, and the individuals impacted are located in various states, a national policy is needed. Security problems have been occurring at banks, schools, government entities, and retailers. This means that any legislation must encompass a broad array of entities.

The bills introduced by Senators Specter and Feinstein are excellent proposals to address the problem, but any such legislation must include language that requires disclosure of an organization's privacy statements and notification policies in an easily readable format. The statement should inform all citizens of what information is being collected and the organization's privacy policies and practices. Monitoring systems should be mandatory, especially for firms that specialize in the collection of consumer data. Victim protection assistance must be included to provide consumers with easy access to credit reports and credit monitoring services. Provisions must also be included to require entities that maintain data to take all reasonable steps to destroy customer records within their control when they are no longer needed by the entity. Finally, high-level executives should be required to certify the monitoring systems and policies in place regarding the accuracy of the notification disclosures.