

# **Position Paper: Toward One Strong National Breach Disclosure Law – Justification and Requirements**

William Yurcik Ragib Hasan

National Center for Supercomputing Applications (NCSA)  
University of Illinois at Urbana-Champaign (UIUC)  
<{byurcik,rhasan}@ncsa.uiuc.edu>

## **ABSTRACT (OUR POSITION IN BRIEF)**

State laws in the U.S. have been very helpful in illuminating breaches of private information by requiring private disclosure between the organization with the breach and the individual owners of the private information that was breached. Although there are currently no public disclosure requirements, these breaches have often been subsequently reported in the mass media.

However, as more states are adopting breach disclosure laws, problems and loopholes are arising that beg a uniform federal law. For instance, state breach disclosure laws do not have uniform requirements so networked organizations must comply separately with each state law – Internet businesses must comply with all state breach disclosure laws. Also state disclosure laws have different triggers and timing that allow organizations to delay or even forgo notification of the same breach in different states.

Our position is that a strong national breach disclosure law is needed in the U.S. to provide uniform requirements to all organizations as well as mandating meaningful public disclosure of all breaches. Such a federal law would eliminate compliance problems between different state laws and provide a valuable tracking mechanism for continually improving the protection of private information.

**Keywords:** privacy information breaches, breach disclosure laws

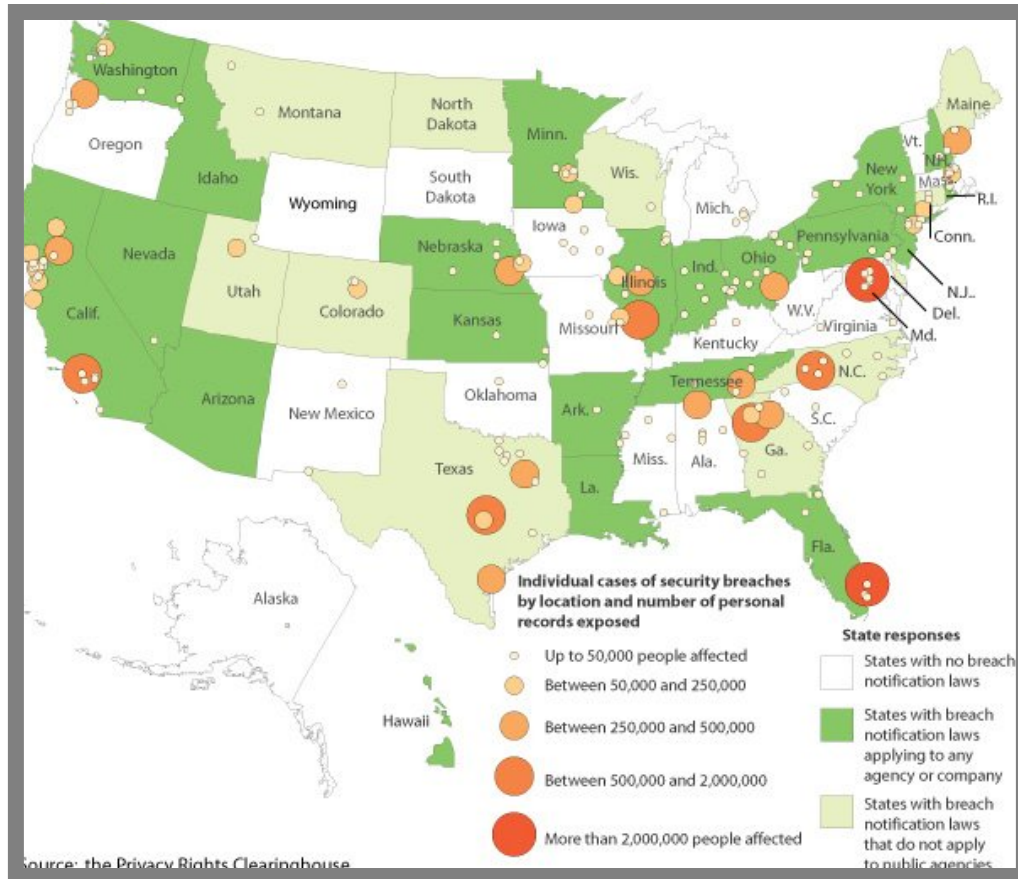
## **INTRODUCTION**

Typical state breach disclosure state laws require direct notification between the third party organization with the compromise and each affected individuals -- without involvement from federal/ state regulators or any level of law enforcement. Private information is defined to be any of the following: social security numbers, driver's license number, bank account numbers, credit/debit card numbers, as well as any other personal identifying information.

State disclosure laws are a significant improvement because affected parties would be unaware of their increased risk of identity theft and the public would not know of the size of the problem through mass media reports [4,5]. However, there are problems. Organizations must assess which state disclosure laws apply to them, a nontrivial task since whether subject to a state law may depend on the location of an organization and/or the residency of those individuals affected [3]. Although state disclosure laws can be categorized into similar groups, each law may have different requirements for notice trigger, timing, content, and recipients.

For an example of the complexity of the problem, some state breach laws require monitoring (per industry best practices) so an organization is vigilant to privacy breaches when they occur. Other state laws require no monitoring. In the states that require monitoring, the type of monitoring is broadly defined giving organizations wide discretion. Rigorous monitoring may detect more breaches and compel more disclosures under state laws. A low level of monitoring significantly below industry best practices may risk customer/shareholder lawsuits and/or fines from state or federal regulatory agencies (state attorney general, Federal Trade Commission, etc.).

### CURRENT STATE DISCLOSURE LAWS (CIRCA JULY 2006)



**Figure 1.** Mapping of Privacy Breaches and State Breach Disclosure Laws {graphic by Danny Dougherty/Stateline.org, used with permission}

California was the first state with a breach disclosure law in 2003. Since then 33 states have enacted such laws. Since 2005, these laws have resulted in notification of 200+ privacy breaches that would otherwise have been unknown. Figure 1 maps disclosed privacy breaches and state breach disclosure laws to show breaches are clustered in urban areas where most organizations are based (although no relation to where and how the breach occurred). Note the anomaly of some states with no disclosure laws which have reported breaches – this is the case where an organization based in a state with no breach disclosure law has a breach event affecting customers based in state with a breach disclosure law (e.g. California), thus required to disclose per California law although not required to disclose in their own state. This is a frequent occurrence that will likely result in jurisdiction litigation and another example of the need for a uniform national law.

## FEDERAL LEGISLATION

Table 1 is a summary of legislation considered by the US Congress during the last three sessions. There has been much activity toward a national law with many variations on a theme. Some legislation focuses on simplifying notification procedures which vary widely per state, other legislation seeks to preempt state breach laws altogether with new requirements. Privacy advocates are concerned about a national law with less stringent requirements preempting strong state laws. Corporate advocates are concerned about the costs of notification versus benefits [1] and desensitization due to numerous notifications [2].

**Table 1.** Recent Federal Breach Disclosure Legislation Being Considered in the U.S. Congress

<b>Proposed Federal Legislation</b>	<b>S/HR Number</b>	<b>Congress (Sponsor)</b>	<b>Disposition</b>	<b>Details</b>
<i>Consumer Data Security and Notification Act of 2005</i>	HR 3140	109 <sup>th</sup> (Bean)	6/30/05 referred to House Committee on Financial Services	directs FTC to establish notification regulations for consumer reporting agencies
<i>Personal Data Privacy and Security Act</i>	S 1789	109 <sup>th</sup> (Specter)	9/29/05 referred to Committee on the Judiciary	requires notification of individuals affected by a security breach and establishes fines and imprisonment for concealment
<i>Data Accountability and Trust Act</i>	HR 4127 IH/RH	109 <sup>th</sup> (Stearns)	5/26/05 report from Committee on Judiciary with an amendment	brokers must submit their security policies to the FTC in conjunction with a notification of a breach followed by an audit
<i>Information Protection and Security Act</i>	S 500	109 <sup>th</sup> (Nelson)	introduced 3/3/05	requires information brokers to protect private info and mitigate any potential harm
<i>Consumer Access Rights Defense Act (CARD) of 2005</i>	HR 3501	109 <sup>th</sup> (Carson)	introduced 7/28/05	financial svc providers to notify customers of unauthorized use of personal information
<i>Consumer Notification and Financial Data Protection Act of 2005</i>	HR 3374	109 <sup>th</sup> (Latourette)	introduced 7/21/05	uniform/timely notification to those whose personal information has been compromised
<i>Financial Data Protection Act of 2005</i>	HR 3997 IH/RH	109 <sup>th</sup> (Latourette)	5/4/06 referred to Comm. on Energy & Commerce	consumer reporters must provide breach notice to Secret Service, functional regulators, involved third parties, & consumers; restore security of information & improve safeguards after a breach; provide consumers free file monitoring
<i>Comprehensive Identity Theft Prevention Act</i>	S 768	109 <sup>th</sup> (Schumer)	4/12/05 referred to Committee on Commerce, Science and Transportation	notification in case of unauthorized acquisition of personal information, establishes an Office of Identity Theft within the FTC for enforcement.
<i>Identity Theft Protection Act</i>	S 1408	109 <sup>th</sup> (Smith)	7/28/05 Committee on Commerce, Science, & Transportation, ordered with an amendment	requires notification in cases of security breaches affecting 1K individuals or more. Preempts state action. Establishes a working group to develop best practices.
<i>Notification of Risk to Personal Data Act</i>	S 751	109 <sup>th</sup> (Feinstein)	7/21/05 consideration in Committee on the Judiciary	notify individuals whose information was obtained by an authorized person, Federal agencies are exempt.
<i>Notification of Risk to Personal Data Act</i>	HR 1069	109 <sup>th</sup> (Bean)	5/13/05 referred to subcommittee on Financial Institutions and Consumer Credit	requires financial institutions to notify affected customers, law enforcement, and a clearinghouse (established by FTC) where a breach of personal information is reasonably believed to have occurred
<i>Identity Theft Notification and Credit Restoration Act of 2003</i>	HR 3233	108 <sup>th</sup> (Gutierrez)	10/2/03 referred to Committee on Financial Services	financial service providers to notify customers of unauthorized use of personal information.
<i>Identity Theft and Credit Restoration Act of 2003</i>	S 1633	108 <sup>th</sup> (Corzine)	9/17/03 referred to Committee on Banking, Housing, and Urban	financial service providers to notify customers of unauthorized use of personal information.
<i>Identity Theft Consumer Notification Act</i>	HR 5474	107 <sup>th</sup> (Kleczka)	10/7/02 referred to Subcommittee on Financial Institutions and Consumer Credit	amends Gramm-Leach-Bliley to protect customers of stolen identities.

Federal Laws already exist with information security requirements specific to particular industries; specifically Gramm-Leach-Bliley (GLB) (financial) and HIPAA (health care). These federal laws require periodic reporting directly to federal regulators with sanctions for non-compliance. However, current federal laws do not have explicit breach disclosure requirements although organizational security status is part of many reports to federal regulators [6]. It is our experience that organizations subject to GLB and HIPAA are careful to hide breach information in security status reports since it is not explicitly required.

## REQUIREMENTS FOR A STRONG NATIONAL DISCLOSURE LAW

A national disclosure law is needed for uniform requirements in the following areas:

Trigger Event: some states require the organization with the breach to themselves determine if the compromised private information is “likely” to result in identity theft. Not surprisingly this has resulted in some organizations not reporting breaches which most objective observers would consider likely to result in identity theft. Other states have a trigger depending on the number of people affected (for instance greater than 1,000 people). Other states exempt certain organizations from having to report. A national law should require all organizations to report all private information breach events.

Timing: States require notification following a trigger event over varying periods of time. A standard time should be set that is long enough for an organization to clearly determine the mechanism and extent of the compromise and also short enough so affected individuals can be warned in enough time to protect themselves from increased identity theft risk. We propose a notification timing of 10 days from the trigger event (based on our experience in security operations).

Monitoring and Enforcement: Some states require organizations to monitor their systems to be able to better determine breach events but, as stated previously, the type of monitoring required is vague and changes dynamically. A national breach disclosure law should eliminate the requirement for monitoring but have a significant civil/criminal penalty if a breach is exposed that was not first reported by the organization.

Type of Notification: Notification should be written using two-day delivery (not electronic nor telephone).

Notification Information: the following information needs to be reported for all breach events to both the affected individuals *and a public clearinghouse* (at present only part of this information is required in many states): (1) number of records breached, (2) type of private information compromised, (3) breach mechanism, (4) number of people affected, (5) estimated cost of breach damage, (6) steps taken to prevent breach from reoccurring, and (7) steps for the affected individual to protect themselves from increased identity theft risk specific to this event.

## REFERENCES

- [1] J. Brandon, “Breach Laws: Rising Security Threat Require Tougher Notification Laws, But at What Price?” *Processor*, Vol 28 No 36, September 8, 2006.
- [2] F. H. Cate, “Another Notice Isn’t (the) Answer,” *USA Today*, February 27, 2005.
- [3] S. Ham, “Internet Privacy: The Case For Pre-Emption,” *Center for Democracy and Technology* (last accessed October 2006) <<http://www.cdt.org/privacy/ccp/statepreemption2.shtml>>
- [4] R. Hasan and W. Yurcik, “Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work,” *Workshop on the Economics of Securing the Information Infrastructure (WESII)*, 2006.
- [5] R. Hasan and W. Yurcik, “A Statistical Analysis of Disclosed Storage Security Breaches,” *ACM 2<sup>nd</sup> International Workshop on Storage Security and Survivability (StorageSS)*, 2006.
- [6] P. M. Schwartz and E.J. Janger, “Notification of Data Security Breaches,” *Michigan Law Review*, Vol. 105.