

Keep Consumers' Personal Data Safe Across State Boundaries

To reform outdated state data breach notification (DBN) laws, America needs to adopt a national DBN framework to provide one-stop shopping and clear rules for notifying consumers when their personally identifying information (PII) has been breached, eliminating regulatory uncertainty for small and medium-sized businesses (SMBs) that make up the vast majority of our Internet-based economy.

We live in a world where people, devices and data are all in a state of mobility. People move seamlessly across state boundaries with the expectation to access their devices and data for a variety purposes. Whether it is to shop online, schedule a dinner reservation, or participate in a video conference call, people have an expectation that no matter where they are, so long as they have a device and an Internet connection, their personal data should be protected – regardless of their geographic location.

However, state laws have not kept pace with technological innovation. Specifically, state Data Breach Notification (DBN) laws that were first enacted as early as 2003, during a time where people only accessed the Internet from their stationary desktop computers, are in some ways relics from a bygone era. These laws generally require businesses to notify consumers that their personally identifiable information (PII) has been breached or disclosed to unauthorized individuals. The laws were not designed to take into account that people, devices and data are in a continual state of mobility without regard for state boundaries.

The first state DBN law was enacted by California in 2003 in response to rapid growth of the Internet. In the early 2000s, the developing Internet was not nearly as dynamic as the interconnected network that exists today. Few people expected the mobile explosion that has taken hold of the IT economy. People and data were less mobile, and desktop computers were the main source of data storage and Internet access.

According to a report by the Pew Internet and American Life Project titled "Internet Adoption Over Time," in 1995, only 14 percent of the U.S. population was "going online." By 2003, the number had jumped to about 45 percent. Consumers were migrating to the Internet by the millions, and from the comfort of their desktops, they were willing to provide PII to conduct e-commerce and pay bills.

Because of the sensitive nature of information or data that consumers share with businesses, California recognized that providing consumers with notice of a breach was a basic and fundamental consumer protection right. Every consumer deserved notice whenever his or her PII was breached. Today, there are now more than 47 state-specific DBN laws in effect across the country, which has resulted in a quagmire of regulatory confusion for businesses that may suffer a data breach of customer data.

WHITE PAPER



Today, there are now more than 47 state-specific DBN laws in effect across the country, which has resulted in a quagmire of regulatory confusion for businesses that may suffer a data breach of customer data.

The World Today

Today's mobile nature of people, devices and data further complicate the patchwork of state DBN laws. In 2012, [Google published a report](#) showing that there are now more than one billion people using mobile devices to access the Internet, surpassing the PC as the primary means of online access. Yet consumers and SMBs are all still operating under a regulatory framework that was created for a technology platform from 2003.

The onward march of technological innovation is unrelenting as evidenced by the emergence of cloud computing which deems state DBN laws even more unworkable. Cloud-based services have eliminated the need for consumers and businesses to store data on servers, and mobile devices allows consumers and businesses to access information that is remotely located, stored and transmitted anywhere in the world. In short, cloud computing services have, in combination with the growth of mobile devices, spawned the age of mobility.

This new and continuously evolving age of mobility will continue to push state DBNs further back in time until they are completely obsolete.

The Problem

What started 10 years ago as an effort to ensure consumers received notice about a breach to their PII has turned into a complicated quagmire – a patchwork of state DBN laws that complicates the notice process for consumers and adds an unnecessary regulatory barrier for SMBs.

For example, state DBN laws vary as to when a consumer notice should be provided. Some state DBN laws require consumer notice when a company is made aware of a breach. Other state DBN laws require notice only if the breached data has the likelihood of resulting in harm to the consumer. Moreover, all state DBN laws differ on the type of penalties and fines that can be imposed and whether a consumer can file a private right of action against a company that has suffered a breach of consumer PII.

Under the current state-by-state DBN regime, there are various scenarios in which state data breach laws do not help the consumer and create regulatory uncertainty for SMBs. For example, what happens when a California resident traveling out of state on business shares his or her PII and credit card information with a website to buy something via a mobile device and the PII is subsequently breached or compromised?

Under California's DBN law "any person or business that conducts business in California . . . shall disclose any breach of the security of the system . . . of any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under this scenario, an SMB may have no way of knowing their compliance obligation. If an SMB has any business ties to California, it may have to unknowingly comply with California's DBN law even if the breach occurred out of state, so long as the consumer is a California resident.

If the breach occurs in Florida, then the rules become even more complicated for an out-of-state resident. [Under Florida's state DBN law](#), a consumer data breach notice is not required "if, after an appropriate investigation or after consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed."



A recent Symantec report shows that the organizational cost for a data breach event is \$5 million and the cost to an organization for a single breached record is \$194.

If a Massachusetts resident shares PII with a website while traveling out of state, then the business that suffered the breach would be subject to the compliance and notice obligations of the state of Massachusetts. [The state DBN law here](#) “applies to any business entity or person that owns, licenses, maintains or stores ‘personal information’ of any Massachusetts resident, regardless of where the entity or the personal information is located.”

Since each state has different notice obligations, the average consumer who is the victim of a PII breach faces a herculean task tracking down where the breach occurred and whether he or she should expect notice from a business with the details of the breach. If a data breach was the result of information provided while traveling and using a mobile device, then the notice obligations will be unclear and muddled at best. This is a terrible scenario for the consumer and for SMBs with an online presence.

The Solution

The dynamic nature of our mobile economy creates the need for a national DBN framework that can provide consumers and SMBs with consistency and predictability on how consumer notice must be and is provided. This means that consumers receive timely notice and details to inform them that a breach of their PII has occurred, and an SMB can be confident that they are in compliance with their notice obligations should they suffer a breach of customer data.

For these reasons, state DBN laws should be a thing of the past. This is not to say that DBNs are no longer needed. Consumer notice about a breach of PII is a fundamental consumer right that must be protected. However, a national DBN framework is the most logical and efficient model.

A significant cost of data breaches results from the regulatory quagmire and patchwork of state DBN laws that cannot be easily deciphered. SMBs must hire lawyers and other experts to help them understand their compliance obligations. For an SMB, hiring a lawyer just for DBN compliance can be prohibitively expensive.

A recent Symantec report shows that the organizational cost for a data breach event is \$5 million and the cost to an organization for a single breached record is \$194. For an SMB, these costs can be intimidating, and serve as a disincentive to expanding services to a wider consumer base. The prospect of being exposed to \$5 million in costs as a result of a data breach incident could in fact sink some tech SMBs.

As consumers and SMBs continue to adopt new and ever-evolving mobile platforms, we need to update our rules of the road. A national framework for data breach notification will help them do so.

A national DBN framework is the most logical and efficient model.



About CompTIA

CompTIA is the voice of the world's information technology industry. Its members are the companies at the forefront of innovation; and the professionals responsible for maximizing the benefits organizations receive from their investments in technology. CompTIA is dedicated to advancing industry growth through its educational programs, market research, networking events, professional certifications, and public policy advocacy. Visit www.comptia.org.

About TechVoice

TechVoice is a partnership of CompTIA, the Technology Councils of North America (TECNA), and participating regional technology associations. Collectively, TechVoice represents thousands of technology companies across the country employing millions of workers. TechVoice is dedicated to empowering and mobilizing the grassroots tech community to impact legislative and regulatory issues important to growth, innovation and job creation. For more information, visit www.techvoice.org.

CompTIA

**Washington D.C.
Public Advocacy Office**

CompTIA Member Services, LLC
515 2nd Street, NE
Washington, DC 20002

www.comptia.org

© 2013 CompTIA Properties, LLC, used under license by CompTIA, Inc. All rights reserved. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. June 2013 A2711-US