

Contending with California Privacy Legislation

Minimizing Exposure to A.B. 1950, S.B. 1, and S.B. 1386

Executive Summary

Whether an institution is based in California or not, if it does business with or stores the personal data of even one California resident, the implications of several pieces of California privacy law can be profound. This document outlines several rules enacted in California that target data privacy, and describes a solution that helps organizations address today's critical security threats and the increased exposure presented by California legislation.

State Laws with Global Implications

Organizations that store or manage the personal data of California residents are being compelled to rethink the ways they guard this information. While the costs of data theft have already been steep, several pieces of California legislation are serving to up the ante when it comes to the repercussions of security breaches, both from a legal, financial, and brand awareness perspective.

Following is an overview of a few of these mandates:

California's Database Security Breach Notification Act, S.B. 1386

Passed in 2002, this law provides strict requirements for notification of consumers following any breach of unencrypted personal data. This includes any combination of an individual's name and such data as credit cards, social security numbers, driver's license numbers, and other information.

California Financial Information Privacy Act, S.B. 1.

This rule, which took effect in July of 2004, imposes steep fines for the disclosure of personal financial information. This law covers both intentional sharing of private financial information as well as the disclosure of data as a result of negligence or security breaches. Fines of up to \$500,000 may be

assessed in the case of a large-scale breach.

California's General Security Standard for Businesses, A.B. 1950

This rule, which took effect in January 2005, requires organizations that manage personal information to implement security procedures to safeguard that data. This law offers definitions of personal data and states that business managing that information must "implement and maintain reasonable security procedures and practices" in order to protect that data.

While enacted in California, the reach of these pieces of legislation is extremely widespread, potentially affecting any organization that does business with, or in any other way stores or manages the sensitive data of, a California resident.

This document will outline how these legal mandates are placing a premium on ensuring data privacy, and it will detail how Ingrian™ DataSecure™ Platforms can help organizations address these mandates.

The Challenge: Ensuring Data Privacy

Just about every sizable enterprise has implemented perimeter security defenses like firewalls and intrusion detection systems. However, the prevalence of data thefts from internal sources, and the fact these perimeter technologies simply aren't foolproof, illustrate that these

technologies aren't enough. Today, comprehensive measures need to be taken to ensure data is secured inside the enterprise, which is where the bulk of personal information resides, and where the most devastating thefts occur. To address these threats and minimize the exposure to the impact of California legislation, organizations must ensure data privacy inside the enterprise.

Achieving Data Privacy with Ingrian

Protecting Data Privacy with Granular Encryption

S.B. 1386 specifies that organizations must “disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

Clearly, encrypting sensitive data is one of the keys to achieving S.B. 1386 compliance, as well as a range of other mandates. Ingrian Networks offers a comprehensive way to encrypt and protect sensitive data at all times, throughout the enterprise. Ingrian DataSecure Platforms provide an intelligent, cost-effective way to protect critical from both internal and external threats. As a result, organizations can better ensure that they are compliant with legislative and policy mandates for security, and eliminate the risks of data thefts. Ingrian's breakthrough solution features dedicated hardware appliances and patent-pending cryptography software.

DataSecure offers flexible implementation options so

organizations can deploy in a way that makes sense for their business and security needs—whether at the Web, application, or database level. DataSecure platforms can be efficiently integrated in Windows, Java, Linux, and Unix environments, and they work seamlessly with leading databases—including IBM DB2, Oracle, and SQL Server. DataSecure encrypts data in databases and applications at the field or column level, and can be used to secure such data as credit card numbers, social security numbers, passwords, account balances, and email addresses.

Intelligently Protect Sensitive Data

S.B. 1386, S.B. 1, and A.B. 1950 all provide some specific definitions of personal and financial data, which generally constitutes a combination of name and such details as driver's license number, social security number, credit card number, etc. The reality is that these records are a very small percentage of the volumes of data an enterprise typically manages, but constitute the most critical threat to an organization if that data gets into the wrong hands.

With its granular encryption capabilities, DataSecure enables organizations to protect only the sensitive data that poses a business or liability risk. Further, by implementing encryption with Ingrian, organizations can ensure that sensitive data is secured...

- at rest in databases and servers, and
- as it is saved to storage systems, including network-attached storage and storage area networks.

Additionally, because they deliver the ability to encrypt at the

application and database layer, DataSecure platforms provide protection against a broad range of threats, including application compromise, malicious DBAs, and storage system security breaches.

Beyond Encryption: The Benefits of a Dedicated Security Platform

Encrypting data alone isn't enough to ensure complete data privacy. For example, if encryption is managed on application servers, data still may not be secure. These servers simply weren't designed for security: they are relatively easy to access, are often misconfigured, and aren't kept up to date with the latest security patches. While encryption can help prevent data theft, ultimately your data is only as safe as the keys that protect it. Whoever has access to the keys has access to your data. And once an attacker has the key, it's relatively easy to copy, modify, hijack, or destroy sensitive information.

According to SB 1386, a breach is defined as “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.” In other words, organizations need to guard not only against theft, but tampering or disclosure, of personal data.

To efficiently protect against these threats, the management of encryption needs to take place on specialized security platforms. By centralizing all cryptographic processing, key management, logging and auditing, and security

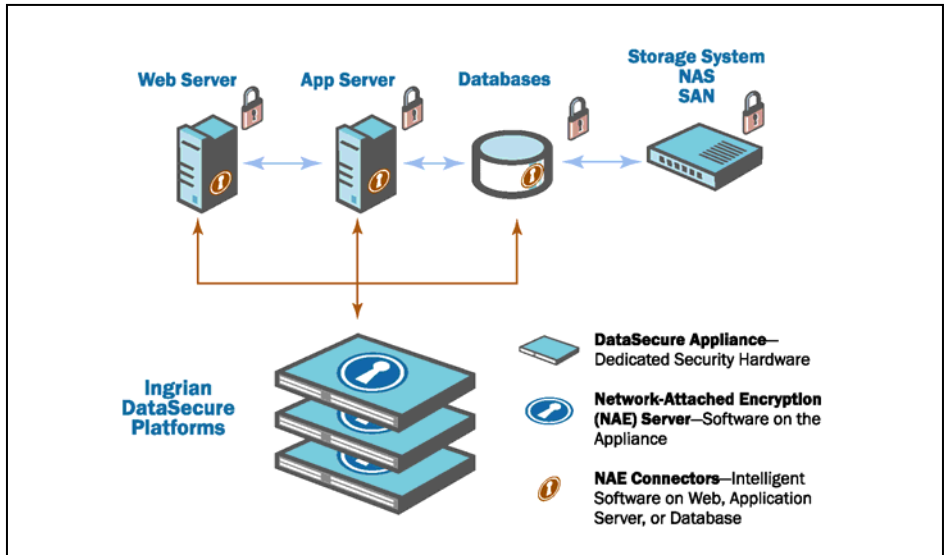
policies on a single, hardened appliance, DataSecure delivers benefits in administration, performance, and, most importantly, security. For example, the cryptographic keys needed to decrypt sensitive data never leave the DataSecure appliance. Also, the appliance can be configured with a variety of administrative safeguards to ensure only appropriate administrators can access the device.

DataSecure features:

- Centralized key management, offering both physical and administrative safeguards—including a FIPS 140-2 Level 3 compliant hardware security module for tamper-resistant protection of cryptographic keys.
- Capabilities for segregating administrative duties so key controls are shared among multiple administrators.
- Secure, multi-factor authentication and access control between databases and servers and the DataSecure platform.
- Granular authorization capabilities that enable constraints to be placed on user operations based on specific key permissions.
- Active alerting capabilities so that, if attempts to breach protected data occur, mechanisms are employed to alert administrators.
- Comprehensive, secure, and centralized logging and auditing of all cryptographic functions and access.

Address Critical Threats and Privacy Legislation—Cost Effectively

Organizations need to address heightened security risks and exposure, while typically contending



with scarce budgets and resources. Ingrian offers a solution that addresses these security risks, while enabling organizations to deploy the platform quickly and more fully leverage their existing resources.

DataSecure can be integrated wherever an organization’s security and business needs dictate—whether at the Web server, application server, or database layer. DataSecure offers support for leading, standards-based cryptographic algorithms: AES, 3DES, RSA, and others. Accessible via standard APIs, DataSecure can be effectively integrated with:

- All Web servers, including Apache, Tomcat, Resin, Microsoft IIS, and others.
- All application servers, including those from BEA, IBM, Microsoft, Oracle, and Sun.
- A range of databases, including IBM DB2, Oracle, and Microsoft SQL Server.
- Legacy and custom environments via an XML, JCE, MS-CAPI, .NET, or PKCS#11 interface.

Automated Integration

With its automated database integration capabilities, DataSecure can be implemented with complete application transparency, dramatically reducing the time and costs normally associated with encrypting data in the enterprise. With DataSecure, administrators can, via an intuitive graphical user interface, make initial configuration settings, then harness capabilities that automate:

- Database schema changes.
- Migration of selected fields from cleartext to ciphertext.
- Installation of triggers and views for application transparency.
- Key rotation to adhere to defined security policies.

In addition, DataSecure can be integrated with bulk load utilities to handle large batch processing and existing data import/export processes.

Ease of Administration

The Ingrian DataSecure platform delivers unrivaled features for streamlining and reducing the costs of ongoing administration—particularly compared to server-based cryptography and key

management. This is achieved through the following:

- Easy-to-use, intuitive management via a graphical user interface.
- Centralized management of all policies, users, and cryptographic keys.
- Automated replication between Ingrian products.

Scalability and Reliability

DataSecure centralizes all cryptographic processing on a highly specialized appliance that delivers performance robust enough for the most demanding batch processing and high-volume online transaction processing environments. A single platform can handle up to 2000 cryptographic requests per second, and Ingrian makes it easy, through load balancing capabilities, to add additional appliances and boost scalability as performance needs dictate.

Further, by offloading CPU-intensive cryptographic processing from disparate servers and databases, DataSecure restores server and database performance to optimal levels—resulting in less waiting for information and higher resource utilization. Designed specifically for business-critical processing, DataSecure offers an array of features to ensure reliability and availability:

- High availability. Featuring

redundant power supplies, fans, and processors on each appliance, DataSecure also enables the use of redundant, replicated appliances and failover configurations that ensure optimal up time.

- Health checking. Web servers, application servers, and databases can determine immediately if an appliance is unavailable and switch to an alternate.
- Disaster recovery capabilities. Enables a second, active site with duplicate, secure backups of critical configuration, policy, and key information—and secure recovery through Ingrian’s FIPS k-of-n smart card recovery mechanism.

About Ingrian Networks

Ingrian Networks brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration, and centralized security management, DataSecure enables organizations to guard against a range of security threats, with unparalleled ease and cost effectiveness. Ingrian is a privately held company backed by such investors as Globespan Capital Partners (formerly JAFCO Ventures), Prism Venture Partners, HighBAR Ventures, and Partech International. For more information, visit www.ingrian.com.

For More Legislative Information

To view complete text of these bills, see the urls below:

- **S.B. 1386.** http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.htm
- **S.B. 1.** http://info.sen.ca.gov/pub/bill/sen/sb_0001-0050/sb_1_bill_20030828_chaptered.html
- **A.B. 1950.** http://info.sen.ca.gov/pub/bill/asm/ab_1901-1950/ab_1950_bill_20040929_chaptered.html

ca1-sb-2005-01