Technology Guidelines for Meeting State Consumer Privacy Regulations

Encrypting and Protecting Personal Information Outside the Corporate Network

GLOBALSIGN WHITE PAPER

GMO GlobalSign Inc

www.globalsign.com

CONTENTS

EXECUTIVE SUMMARY

As the security threat landscape evolves, state regulators are taking action to hold businesses accountable for protecting the privacy of consumer personal information. Massachusetts has implemented the most stringent consumer privacy regulations to date, requiring businesses to encrypt the personal information of any Massachusetts resident when the information is sent over the Internet or stored on mobile devices such as laptops, or corporate servers and storage devices.

To meet these consumer privacy regulations, businesses must look beyond traditional security measures that focus on perimeter security and applications access within corporate firewalls. Most businesses will need to invest in encryption technologies to address the confidentiality requirements of this legislation.

Many encryption solutions only go partway to addressing the need. Rather than encrypting specific devices or channels, businesses need to focus on encrypting the files that contain consumer personal information. By adhering to six essential guidelines, businesses can meet stringent privacy guidelines for personal information that travels or resides outside of the corporate network:

1. **Focus on encrypting files in transit and at rest.**
2. **Make sure consumers can trust and validate files from your business.**
3. **Insist on flexible access rights.**
4. **Respect the consumer's time.**
5. **Get real-time insight into problems.**
6. **Control access to files containing personal information outside the network.**

Overview: The evolving regulatory landscape

Around the country, states are taking the initiative in protecting consumers from identity theft and fraud, adopting diverse laws that require businesses to demonstrate protection of residents' personal information. And state regulators and attorney generals are stepping up audits and sanctions for violations of data breach regulations.

Two sectors heavily affected by recent consumer privacy protection legislation are the financial sector—including banking, insurance, and financial planning and tax advisors—and the healthcare sector. But companies in every industry, and of all sizes, are subject to these state regulations guarding consumer privacy.

Of the state regulations to date, Massachusetts has implemented one of the most stringent and far-reaching requirements for protecting consumer privacy for its residents.

The Massachusetts regulation, 201 CMR 17.00, breaks new ground on a number of levels:

***A broader definition of personal information*.** While many states focus primarily on the privacy of Social Security numbers, the Massachusetts regulation has a much broader definition of what constitutes protected "personal information" or PI. Businesses must protect any information that includes the resident's first and last name together with one or more of the following data elements:

- **Social Security number**
- **Driver's license**
- **State-issued ID**
- **Financial account number (including credit or debit card numbers)**

***Broad application*:** The regulation applies to any business that handles personal information for any resident of the state—regardless of the location of the business or the nature of the relationship. For example, a business that employs a contractor residing in Massachusetts would need to adhere to the privacy regulations for that contractor's personal information.

***Explicit encryption requirements*:** While many regulations tend to be vague about specific technologies, the Massachusetts law requires that businesses encrypt personal information sent over the Internet or stored in laptops or portal devices. These requirements state that the information itself must be encrypted, not the method

of delivery. In addition, businesses must monitor files containing personal information for unauthorized access.

Clearly this regulation presents challenges for businesses of all sizes. But the compliance effort pays off over time, as businesses that can comply with 201 CMR 17.00 will be in a good position to comply with others states' privacy and data breach regulations as well.

Full compliance with 201 CMR 17.00, and the other state regulations, encompasses people, processes and technology. Businesses need a Written Information Security Plan (WISP). They need to designate someone responsible for it, and to train employees. Massachusetts has published a checklist that can be helpful for businesses looking to comply: **http://www.mass.gov/Eoca/docs/idtheft/compliance_checklist.pdf**

This paper primarily considers the regulations so far as they cover electronic information outside of business networks.

The world isn't as simple as it once was

Today's IT and business environment is much more complex than it was even five years ago. The security strategies and best practices established over time are insufficient to address the challenges of protecting personal information in today's business environment, for several reasons.

Expanding virtual boundaries. With a broad definition of what constitutes personal information, chances are that customer and employee information often leaves the boundaries of your business network.

- **As businesses adopt cloud-based services and collaborate with partners and suppliers online, the boundaries of the corporate network become irrelevant.**
- **Employees rely on mobile devices to take their work with them on the road and at home. Many files will include regulated personal information in various forms.**

Traditional security measures have focused on securing access to applications, networks and systems, and to creating 'secure channels' for data transmitted between entities. Perimeter security measures like firewalls and intrusion prevention systems are essential to corporate network security, but insufficient for today's environment. The "perimeter" you are trying to defend is vague at best, and highly permeable.

Online interactions with consumers. To secure your customer's personal information, you must secure interactions all the way to the consumer's browser and beyond to where the data finally resides. And because the consumers are current or prospective customers, any security and privacy measures cannot negatively impact their interactions with you. It is harder to impose security and privacy policies on customers than employees. There's a delicate balance between respecting consumer privacy and making it difficult for consumers to do business with you.

Duty to report breaches. Most state regulations include a timeframe for reporting breaches of consumer privacy. Unfortunately, it may be difficult for businesses to know that data has been compromised, particularly when the event occurs outside the corporate network. Timely insight is important; by spotting problems quickly, you can often correct them before they escalate. In addition, some regulations like the HITECH act exempt organizations from notifying consumers if the breached information was encrypted according to NIST standards.

Breach notification

According to the National Conference of State Legislatures, 46 states plus the District of Columbia, Puerto Rico and Virgin Islands now have laws requiring notification for personal information security breaches.

Diverse file types. Regulations like the Massachusetts law apply to consumer personal information in any file type. It's not enough to lock down databases and use secure email—personal information may reside in many types of files, such as spreadsheets, legal contracts and presentations. Any solution that protects and encrypts

data must be able to handle a broad range of file types, including Microsoft Office documents, Adobe PDF, and XML to name a few.

Encryption is an essential part of compliance

For most businesses, complying with consumer privacy regulations will require some level of technology investment. Most businesses have solved the problem of encrypting data in transit, using SSL and secure email with the S/MIME standard. But encrypting data at rest, on laptops, mobile devices, and computer hard-drives will require new technology investments for most businesses.

In choosing encryption solutions, businesses have to determine how to meet privacy mandates without imposing undue burdens on staff or their partners, suppliers and customers. They need solutions that monitor and alert them to access problems, and give them a good deal of control over access to personal information, even when it resides outside the business network.

6 guidelines for choosing encryption solutions

There are many types of encryption solutions available today, including file and disk encryption, database encryption and encrypted email. Many of these solutions address some, but not all, of the requirements of regulations like 201 CMR 17.00.

As you evaluate the encryption technologies your own business should deploy, use the following guidelines to ensure that you address the complexities of today's work and regulatory environment.

1. Focus on encrypting files in transit and at rest.

To address state consumer privacy regulations like that of Massachusetts, you need to broaden your focus to the information itself, in all of its incarnations and locations. You need a way to wrap access control policies and security around the individual files or groups of files containing protected personal information, so that when it leaves the corporate network it remains embedded in your security policies.

Many encryption solutions go partway to addressing the problem. For example:

SSL: This ubiquitous protocol creates a secure channel for communications with customers, protecting information in transit.

Secure email extends the secure transmission to email, using the S/MIME protocols. However, once the email is open on the client, it is free and clear, and you lose control over who accesses the content. In addition, secure email with S/MIME only authenticates the sender of the email, not the person receiving it.

Laptop encryption: This technology, when deployed on employee laptops, protects companies from the ramifications of laptop theft, which may include losses beyond personal information. But it doesn't address the other types of mobile devices where personal information might reside, including flash drives and smart phones. And it does not address the issue of communicating with the consumers themselves, who are unlikely to be using laptop encryption solutions.

Faxing: Like SSL, faxing secures the communication channel, but not the file where it arrives at the endpoint. Once a fax arrives and prints out, its access cannot be tracked, nor its receiver authenticated.

Disk encryption: Even on corporate servers, encryption is only part of the equation. The WikiLeaks incident is a great example of a seemingly secure network that was completely foiled by a single user able to remove countless documents. Securing the network, instead of the information and files themselves, leaves businesses vulnerable to this kind of problem. Encryption without digital rights management is not enough; organizations need to control who gets access to what and when.

Rather than focusing on channels and devices, focus on the files themselves that contain personal information. Choose a file encryption solution—ideally, one that can handle any type of file, from a PDF to a spreadsheet to a Word file. It should handle encryption and convenient decryption for authorized users both within and outside your corporate network. By encrypting a file and restricting

decryption to authorized users, you can control access to that file no matter how it may be delivered or where it comes to rest.

2. Make sure consumers can trust files from your business.

When you send consumers or partners encrypted files for their approval or interaction, they should feel a high degree of certainty that the file originated from your business—particularly if the file contains sensitive personal or financial information. You should be able to demonstrate that the source is a verifiable, trusted identity, and it should be difficult or impractical for someone else to spoof an authentic document from your business.

3. Insist on flexible access rights options.

The file encryption solution should support a range of access control levels that are easy to set on a file-by-file basis, depending on the nature of the information contained in the file, and that authenticate users not only when encrypting data, but when decrypting it as well.

For example, your policies may require strong, 2-factor authentication for users that are encrypting/certifying documents from your business. You should also be able to set different access roles/authentication levels for the recipients who need to decrypt the data. A file intended for a customer may require simple password protection, while others can be restricted to employees of your group or business, or even require strong authentication such as a certificate or biometric for access.

Make sure the solution gives you the ability to align authentication levels with the specific need for the file and usage in question.

4. Respect the consumer's time.

Few consumers really care to understand the intricacies of encryption technology. They simply want to know that you're protecting their data, and they want easy access to it as needed.

Any file encryption solution must be simple use. It should work with any file type or browser, and require minimal effort on the part of the consumer. This is not to say that you cannot require a minimal client application for file encryption and decryption. People are accustomed to the idea of downloading readers or add-ons such as Adobe Flash Player or Adobe Acrobat Reader. But any solution should meet the following requirements:

- **It must be free of charge to the consumer needing to decrypt files.**
- **It must be quick and easy to install, on a wide range of desktop platforms.**
- **It needs to be extremely easy to use.**
- **It must demonstrate its value—consumers should be able to see that you are respecting and protecting their privacy using file encryption.**

5. Get real-time insight into problems

Timely response to problems is critical for regulatory compliance. In addition to making the upfront effort to protecting personal information, you need to know when those efforts may be failing, for whatever reason—even when files are outside of the corporate network.

Choose a file encryption solution that provides real-time notifications of unauthorized access attempts as they happen. With that insight, you can identify data that might be at risk and take steps immediately to remediate the risk. File encryption solutions effectively eliminate breaches to sensitive information as only authorized individuals can gain access, regardless of where the information resides.

In addition, look for forensic auditing capabilities that help you demonstrate compliance with state consumer privacy legislation by providing detailed reports of all activity associated with personal information stored or transmitted electronically. Current audit practices apply equal importance to building security safeguards into encryption systems as to addressing breaches after the fact.

6. Control access to personal information outside the network

Because your business is legally responsible for documents containing consumer personal

information held and transmitted, you need to retain a degree of control over sensitive files, even when they reside outside your corporate network. A file encryption solution can deliver this control, because the client must interact with the encryption server at the time of access to decrypt the file. This means that you have the availability of defining and changing policies for file decryption at the server level, even for files that have left your premises.

The file encryption solution should give you the ability to set a specific deadline for decryption access—for example, 'expiring' the ability to decrypt a file after a specific time period. You should also have the ability to override those policies as needed:

- **Reactivating an expired file if a customer needs it.**
- **Shutting down access to a file if an alert or report indicates that it is the target of unauthorized access attempts.**

SUMMARY

By encrypting and controlling access to files containing personal information, businesses can immediately and cost-effectively address state consumer privacy regulations. Fortunately, file encryption solutions are available today that build on a mature technology and infrastructure foundation, leveraging what we have already learned from SSL and secure email encryption.

By choosing a flexible solution that meets the guidelines listed in this paper, businesses can not only address state regulations, but also protect other sensitive data in an increasingly mobile and virtual work environment.

ABOUT GLOBALSIGN AND BIOWRAP®

GlobalSign is a well established Certification Authority and SSL Certificate Provider. A leader in public trust services since the very birth of the commercial Internet, GlobalSign Certificates are trusted by all popular browsers, operating systems, devices, and applications. GlobalSign's trusted digital certificates allow thousands of authenticated customers to conduct secure online transactions and data transfers, distribute tamper-proof code, and protect online identities for secure email and access control.

GlobalSign, in partnership with NATION Technologies, delivers an advanced file encryption and management solution called BIOWRAP® Certified by GlobalSign that addresses the needs of businesses that must comply with consumer protection legislation, as well as other regulatory requirements for government, financial, insurance and healthcare industries.

The BIOWRAP® solution is an application-based solution that allows users to easily create an unlimited number of truly secure, authenticated, and accountable electronic files using a GlobalSign Digital Certificate. Once a file is encrypted, only authorized recipients can view the file using the Free BIOWRAP® Reader, providing the user with absolute confidence that the file is authentic and unaltered. GlobalSign registered users also have access to real-time forensic auditing reports.

For more information on BIOWRAP®, visit http://www.globalsign.com/file-encryption/ or call your local GlobalSign office.

GlobalSign US & Canada Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com