# TextGuard

## Mobile Electronic Communication Compliance and Security

## The Proliferation of Workplace Text Messaging, Smartphone Use and the Growing Challenge of Mobile Communication Data Security and Compliance

**A White Paper**
**June 16, 2010**

### Texts, IM's and Smartphones – The Future of Business Communications

Text messaging is no longer a phenomenon or the next big thing - it's a way of life. Beginning in the second quarter of 2008, U.S. mobile subscribers sent and received more texts than actual phone calls. In fact, according to Nielsen, text messaging increased 450% between the first quarter of 2006 and the second quarter of 2008. Just how many text messages are being sent and received? Try 2.5 billion per day, as of June 2008.

At the same time that text messaging is surpassing cell phone usage; the use of smartphones in the workplace is increasing exponentially, as well. If you're reading this, you're probably well aware of how many company-issued smartphones you currently have in service. You're also probably aware that more and more employees are asking to access your corporate network from their personal smartphones. According to Forrester Research, half of the smartphones in use in U.S. and Canadian businesses are not company assets.

IDC, a mobile communication research authority, says 80% of small to medium sized business have employee-owned smartphones in use. They go on to predict that, by 2013, 56.7 million business smartphones will be shipped specifically for employee purchase. This goes right along with Forrester Research's prediction that, by 2013 as well, smartphone usage among U.S. information workers will triple.

No longer are just executives, salespeople or field service technicians relying on smartphones to help increase their productivity and keep them in touch with customers' needs. Requests are coming from all ends of your organization to access company email, calendars and CRM applications. Your employees are not just using their smartphones for workplace productivity. They are sending and receiving all types of communications, including text messaging, IM's and eventually mobile voice recordings.

As companies like Microsoft, Research in Motion, Apple, and Google all continue to make connecting employee-owned smartphones to the enterprise easier, the need for increased data security and compliance becomes critical. This need is amplified if your industry is regulated, like financial services

or healthcare, where the archiving of business communications is compulsory. Where do text messages (in the SMS or PIN format), IM's (instant messages or BlackBerry messages), and other forms of communication sent and received by smartphones come into play when discussing proper data security?

## Mobile Electronic Communications – The Need for Compliance and Control

***"Just as cell phone calls are not recorded, neither are text messages.***

***Regular text messages sent through regular cell phones are not kept in any central repository. When you zap them from your phone they are, in almost all instances, forever zapped. There is no federal law requiring that they be stored or kept by the cell phone provider."***

*- Mike Wendland, Detroit Free Press Technology Columnist -*

This quote is exactly why every IT executive, Controller, Chief Legal Officer, CHRO, CFO, COO, and CEO needs to make mobile communication security and compliance a top priority.

The quote is from 2008 and, since then, several mobile carriers have instituted SMS archiving for short periods of time. In addition, software that can recover deleted texts from a smartphone's SIM card is readily available at a reasonable cost. However, there are still no mobile phone providers who offer a total SMS compliance, monitoring and archiving solution as part of their service. In addition, there are no federal laws mandating the preservation of all mobile communications.

Several regulatory bodies require the storage of certain types of business communications. For example, *The Sarbanes-Oxley Act* requires preservation of a variety of business records for specified time periods. The definition of "business records" does happen to include many types of mobile communications, among them text messages and, in some cases, instant messages. What follows are examples from healthcare, financial services and government illustrating the consequences of the failure to properly secure or preserve mobile communications.

### Protecting Patient Information in the Age of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) mandates a patient's health records may not be released to third parties without the patient's written consent. In addition, the law prohibits viewing of patient information by unauthorized medical provider personnel. HIPAA aside, some states have their own privacy laws in place. In June 2010, Ronald Reagan UCLA Medical Center was fined $95,000 by the State of California for failing to prevent unauthorized employees from accessing confidential patient information. This followed a 2009 fine of Kaiser Permanente's Bellflower Hospital for a similar violation of California law.

Imagine the potential consequences of a health care professional disclosing a patient's confidential records via a mobile communication device, without proper consent. Obviously this is a serious violation made even more severe by the health care provider's inability to effectively monitor the mobile communications of its employees, even when they occur over the provider's own secure network. As important as the safe and secure transfer of information is in the healthcare industry, it quite possibly is more important in the financial services sector. Several regulatory bodies, such as FINRA and the SEC, are charged with the monumental task of governing transactions, communications, and behavior in the financial services industry.

### Financial Services – The Cost of Breaching Confidentiality

How many times, in the past few years, have you received a letter from your mortgage company, bank or 401k administrator advising of a security breach and offering a free period of credit monitoring to

protect you against identity theft? This letter generally comes at the end of a lengthy investigation into the particulars of the breach and after FINRA, or another regulator, has levied a substantial fine. In fact, FINRA fined Centaurus Financial, Inc. $175,000 in 2009 for its failure to protect confidential customer information following incidents in 2006 and 2007.

In addition, FINRA fined D.A. Davidson & Co. $375,000 in 2010 for a similar failure stemming from activities that occurred in late 2007. Both companies needed to make substantial changes to their information security systems and processes while providing one to two years free credit monitoring to affected clients. Imagine being the information security or compliance officer charged with reporting the breach to the executive team. Healthcare and financial services notwithstanding, government agencies on all levels also face significant challenges when attempting to monitor mobile communications and insure proper use of smartphones, PDA's and the like.

## Local Government – Privacy vs. Policy

Whether it's a matter of national security, confidential employee information, or proprietary government contract data, securing data and ensuring regulatory compliance is of the utmost importance. The United States Supreme Court has become involved in matters concerning the privacy of mobile communications over government-supplied equipment and networks in the case of Ontario vs. Quon. When The City of Ontario, CA audited Stephen Quon's text messages to insure compliance with a work-use only texting policy, it found sexually explicit messages he'd sent to his wife, his girlfriend and a fellow officer.

The central issue in Quon vs. Ontario is an employee's "reasonable expectation of privacy". Quon prevailed in his 9th Circuit U.S. Court of Appeals case due to the court's interpretation of the *Stored Communications Act*, a section of the *Electronic Communications Privacy Act of 1986*. The *SCA* stipulates that communications stored by a third party cannot be viewed by the employing agency without the consent of the employee. Since the pager's provider stored the texts on their systems and the police department viewed these texts without Quon's consent, the appellate court found the City of Ontario in violation of Quon's 4th Amendment right to freedom from "unlawful search and seizure".

Had the City of Ontario been using technology that allowed them to monitor and archive text messages internally, much the same way they monitored and archived emails, they would've had every right to take action against Sgt. Quon for his violation of department policy. The *SCA* includes a specific exception allowing employers to access communications stored on electronic services they provide.

There's a central theme running through all of these examples. Monitoring and compliance equals control. The right system and the proper implementation keep your mobile communications from creating liability that costs you time and money. Even monitoring and compliance are not enough, though. Here are some examples of the potential consequences when a device is hacked, lost or stolen.

## Protect the Device – Protect the Data

In April 2010, security researchers at the Intrepidus Group hacked into Palm's new WebOS platform using nothing more than text messages. The texts were able to point the O/S's web browser at a potentially malicious web page and open it, as well as turning off the handset's radio. In a similar experiment, two other researchers used texts to take complete control of an iPhone. Imagine someone else being able to make calls, steal data, or send texts from your phone while it's still in your possession. If that sounds scary enough, you may not want to read the next example.

You're an executive in a medium sized insurance company that is owned by a bank holding company. Your company is regulated by your state insurance commission and subject to compliance with SOX, the GLBA, and HIPAA. You're out of town on business and minutes into your taxi ride to the

hotel, you find it odd that your belt hasn't vibrated lately because you're accustomed to receiving calls, emails and texts throughout each day. After a quick check of your luggage, you realize your smartphone is gone.

Upon arriving at your hotel, you notify the airport, your airline, and your employer of the situation. Your risk management folks start working with your company's mobile service provider to deactivate the phone and erase whatever information is stored on it remotely. This process generally takes a few hours. Now it's a race against the clock. Has the airline found the phone? Has it fallen into the wrong hands? What exactly is stored on the phone? Customer information, employee information, proprietary information? What happens if this information falls into the wrong hands before the phone can be shut down and wiped?

Increased use and reliance on smartphones equals increased risk. These risks explode when the time, or navigation of red tape, required to deactivate and invalidate the mobile device is substantial. Can you or your company afford to bear the potential costs of confidential or proprietary information loss or theft?

## Mobile Electronic Communication Security and Compliance – An Ideal Solution

***"Security is always excessive until it's not enough."***

*- Robbie Sinclair*

*Head of Security, Country Energy –*

Any solution to the problem of total mobile communication security must be comprehensive. The solution must be able to monitor, log, archive, or block mobile communications. In addition, it must be able to track the movement of mobile communication devices and secure them in the event of loss or theft. Finally, it must be easy for your compliance team to access the information necessary to properly address security breaches or violations of company guidelines.

Features of the solution aside, it must offer many characteristics that allow it to be implemented easily and integrated seamlessly into your company's network. Scalability, upgrades, and data backup must also be key factors. For example, if your access to information is limited by a third party's hosting of the solution (in the case of government agencies that must abide by the *SCA*), you'll want a solution that can be installed directly on your company's or municipality's existing network. Let's start breaking down the ideal mobile communication security solution in terms of its handling of various types of messaging.

### Message Handling Features

The ideal solution encompasses a variety of different interactions with mobile communications such as SMS, PIN to PIN messaging, email and mobile instant messaging. Each industry will have different requirements and the solution must provide the proper method of handling for each. For example, the *FRCP* (*Federal Rules of Civil Procedure*) was amended in 2006 to make electronic information discoverable. The ideal solution offers data storage in the WORM (Write Once, Read Many) format making changes and deletions impossible.

#### Monitoring

The ability to associate each user to a particular smartphone and subsequently monitor each mobile communication sent and received is paramount. The monitoring function gives your compliance officer the ability to identify potentially dangerous messages and take real-time action to enforce company

policies and limit your exposure. The solution must also allow you to monitor a device in order to verify an employee's location or monitor overall usage to insure employee adherence to company-owned mobile communication device policies.

**Logging and Archiving**

In regulated industries, e-communication archiving is often compulsory. The ideal solution allows unlimited logging and archiving of SMS messages, emails, BlackBerry PIN messages and mobile instant messages. Compliance ceases to be an issue when all mobile communications are automatically logged and archived for easy retrieval whenever they're needed.

**Blocking and Filtering**

Certain types of communications do not belong on your company's smartphones or within the infrastructure that supports them. Being able to configure the solution to filter or block incoming and outgoing texts, emails, calls and web pages keeps inappropriate and potentially harmful content and/or communications from coming into the organization or going out of it. An especially important element of blocking is being able to easily enable it by keyword, domain or sender.

**Flagging and Alerting**

When a protocol has been breached, your compliance and security staffs need to know right away so they can determine the source and decide on the prior response. The ideal solution includes advanced reporting capabilities that provide the ability to send alerts to the right people once any mobile communication has violated protocols. When combined with robust logging capabilities, the ideal solution can flag an inappropriate communication and create an audit log file automatically.

Now let's discuss how an ideal solution should operate to insure easy integration, ease of use, and maximum effectiveness.

## Enterprise Level Features

The ideal solution must have application-wide features that make integration simple, use intuitive, and automation standard. For example, certain groups within companies may not be allowed to share customer information with one another. The ideal solution allows the end user to configure certain ethical boundaries between functional areas and enable alerting should inappropriate mobile communications occur.

Let's discuss some of these necessary features and their benefits to your company and your end users.

**Integration / Compatibility**

The ideal solution works with any mobile carrier or network and is compatible with multiple mobile communication devices and platforms. The solution does not replace the device's built in security features – it enhances them. Some companies have contracts with more than one mobile carrier and with the growing trend of employee-owned devices being connected into the corporate infrastructure; this is an especially important feature with an obvious benefit to both the employee and the company.

In addition, the ideal solution will integrate with the company's current email archiving solution, including its data vault. This creates ease of use and is a more efficient utilization of a company's data storage resources.

**Configuration**

Being able to easily configure a solution to the specific needs of your company and industry is essential. This starts with how the solution is delivered. The ideal solution must be configurable either

as a hosted solution, one that's loaded directly onto your existing network, or a hybrid of the two. This takes your specific needs and limitations into consideration.

Configurable logging and archiving must be available in order to associate each device with a particular user and/or a specific department or business area. Configurable logging and message archiving also sets the proper parameters for data retrieval, enabling a wide variety of advanced searching and record filtering capabilities.

Configurable monitoring and flagging of messages allows the end user to define the variables based on the company's and industry's compliance requirements. With the proper variables defined, the user can then create audit log files and record search activity by department, user, or device as well as being able to create alert criteria. In addition, configurable monitoring and flagging allows for a single user's activity to be recorded across multiple devices and/or formats.

**Usability**

The ideal solution also needs to have an intuitive user interface that puts the power of all its capabilities at the fingertips of an authorized user, usually an IT security or legal compliance officer. Following a secure login, the user should be able to do the following:

- Install the solution on a smartphone or other mobile communication device at the device's keyboard or "over the air"
- Locate, lock and delete the contents of a registered mobile communication device
- Directly access the mobile communication repository to search for messages
- Review and annotate conversations to ensure policy compliance
- Access a variety of reports and create ad-hoc data queries, then export results to multiple file types

**Automation**

A compliance officer cannot maintain complete control over every mobile communication initiated or received by employees. Automation is a key function in any mobile communication security solution. The ideal solution automates reporting functions based on user-defined criteria, like type of communication, user, device, or even keyword. For example, an automated daily report can be queued for an entire division or just one employee who may be considered "high risk".

In addition, regular updates and upgrades must be automated and pushed "OTA" to mobile devices in service as well as pulled from the server to client machines internally connected to the company's network. Laws will change, court cases will change their interpretation and new technologies will be developed. In fact, the solution should be easily upgradable to handle mobile Instant Messaging, BlackBerry Messaging and mobile voice recording. The solution must be able to adapt to these changes and make the upgrade process virtually invisible.

**Encryption / Security**

The ideal solution must insure that all mobile communications are secured by using, at the minimum, SSL encryption technology. Secondly, data backups must be securely encrypted, especially if mirror image records are to be created for web use. Finally, data archives must be secure and unalterable through the use of encryption and WORM.

Another essential security function is remote device control. The ideal solution includes the ability to lock down a device once it becomes lost or stolen, locate the device for tracking and retrieval purposes and erase the information on the device quickly.

**Backup**

Securing data during transmission and at the server level is important but another important element an ideal solution must have is effective data backup. The ideal solution allows backups of contacts and other mobile communication device settings to a remote server and even has the capability to automate them. In addition, the solution enables mirrored storage of archived messages to allow web access for authorized users through an intuitive web interface.

As you can see, the ideal mobile communication security solution combines the following elements to gain total control over mobile communications within your company's network:

- Ease of installation, update and use
- High levels of data and application security
- Configurations to fit your specific monitoring, blocking, alerting and reporting needs
- Robust features including real-time monitoring, advanced search and retrieval, and on-demand ad hoc reporting
- Upgradability to adapt to a changing legal environment and an evolving mobile communication landscape

## The Ideal Solution Exists

*"With the increase in **E-Discovery** and **E-Communication** monitoring and the interpretation of the recent messaging regulations, corporations in the affected sectors must implement secure message monitoring and archiving solutions,"*

*- Todd Cohan -*

There are many products are the market today that offer some of the features discussed above. Some excel at device management, spam blocking, or malware detection – all valuable benefits, of course. Some are just beginning their forays into mobile communication security and their entrance into the market is welcome as by 2013, handheld devices will be the most popular way to access the web. However, only one mobile communication security solution offers you total control over all mobile devices operating on your company network.

### Introducing TextGuard

TextGuard was designed by veterans in the Compliance, Data Security and Information Technology industries to be the premier information security solution for mobile communication devices. After a thorough technical, market and feasibility analysis, TextGuard was created to succeed in a volatile and ever-changing IT marketplace by being a total mobile communication solution with robust features, 24/7 support, and the innovation necessary to become and remain the benchmark in the industry.

This white paper has discussed the elements of an ideal solution for mobile communication security in great detail. So just how does TextGuard measure up?

| Feature | Yes/No | Specific Capabilities |
|---|---|---|

| | | |
|---|---|---|
| Implementation | Yes | TextGuard's client is installed on the device either via keyboard or "OTA" while the server component is either hosted on the web (SaaS) or installed directly to your network based on your company's specific needs |
| Compatibility | Yes | TextGuard works with any mobile carrier and with RIM Blackberry, Windows Mobile and Google Android operating systems; TextGuard handles email, SMS, PIN, Instant Messaging, and BlackBerry Messaging |
| Monitoring | Yes | TextGuard automates monitoring of all incoming and outgoing communications from the smartphone which enables several filtering and blocking options |
| Filtering/Blocking | Yes | TextGuard can selectively block incoming and outgoing calls as well as access to questionable web sites on select operating systems; TextGuard also filters SMS and email for obscene and prohibited content on select operating systems |
| Logging/Archiving | Yes | TextGuard automatically logs and archives every single communication going to and coming from the smartphone and is the only mobile security solution that maintains its logs and archives on a secure server while providing access to authorized users from any location via the web |
| Security | Yes | TextGuard enables administrators to lock a mobile communication device in order to prevent data loss in the event the device is lost or stolen; data can be erased from the device remotely |
| Compliance | Yes | TextGuard's archived messages are stored using WORM technology, making them inerasable and uneditable in order to facilitate their use as evidence; TextGuard's archives also retain messages for as long as you require to meet retention requirements in a number of industries, such as healthcare, pharmaceutical, financial services, accounting, and legal |
| Reporting | Yes | TextGuard's reporting capabilities include the ability to flag messages by keyword and automatically create audit log files; the ability to track all communications from a single user, phone or department; and the ability to create on-demand ad hoc reports or schedule their delivery via email, ftp or file sharing |

This list of features, capabilities, and advantages of TextGuard is substantial, to say the least. TextGuard also offers a 24/7 support portal with a comprehensive knowledgebase, updates and new releases, new user setup, and support ticket handling. In addition, the solution can be customized to your company's specific needs and requirements. Uptime and performance SLA's are your guarantee that TextGuard will perform when it matters most. Finally, every archived message is continuously accessible with absolutely no time limit. You may set the length of time messages are kept based on the specific regulatory and compliance guidelines of your industry.

## Conclusion

We hope this white paper has shed light on the unwanted consequences that can result from the loss or theft of confidential and proprietary data, the grave risks of a poorly defined and executed mobile communication security plan, and your immediate need for a solution that is comprehensive, user-friendly, and built to adapt as new communication technologies (such as smartphone voice recording) are developed.

There can be but one conclusion drawn from the information presented here. TextGuard is the ideal solution for creating an overall enterprise-wide information security regimen for every smartphone in use on your company's network. For more information, visit www.textguard.com.