THINKstrategies

*A Whitepaper for IT/Business Decision-Makers*

# Dispelling the Data Security and Privacy Myths About Cloud-Based, Software-as-a-Service CRM Solutions

## *Why Fears About the U.S.A. Patriot Act & Other Government Regulations are Overblown and Should Not Limit Adoption*

**Published by THINKstrategies, Inc.**

THINKstrategies

# Introduction

The convergence of a series of major macro-market trends has sparked the emergence of a new generation of powerful and cost-effective, web-based solutions which are quickly becoming viable alternatives to traditional, on-premise software and systems.

These new solutions are referred to as Software-as-a-Service (SaaS) and Cloud Computing. They offer an 'on-demand', 'pay-as-you-go' alternative to the upfront costs and complexities associated with 'legacy' systems and software.

The ease of deployment and use of these cloud-based services also makes them more user-friendly, productive and cost-effective than the cumbersome and costly on-premise systems of the past.

Yet, despite the growing examples of organizations gaining tangible and measurable business benefits from SaaS solutions, many corporate decision-makers are apprehensive about adopting these cloud-based services because of concerns regarding data privacy.

They are particularly concerned about using services delivered by U.S.-based providers because of the ominous language contained in the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, commonly referred to as the U.S.A. Patriot Act.

This regulation appears to permit U.S. law enforcement agencies to unilaterally access private customer records stored on corporate servers worldwide if they are suspected of holding data which could pertain to terrorist threats or other criminal activity.

These fears have made some organizations especially hesitant to consider SaaS-based Customer Relationship Management (CRM) software and services offered by U.S.-based SaaS vendors, since these systems serve as a short- or long-term storage area for sensitive customer information.

THINKstrategies believes these risks have been overly exaggerated and raise unfair questions about doing business with U.S.-based companies. Ironically, companies who avoid contracting with leading U.S. SaaS providers may be at greater risk of data privacy breaches by continuing to rely on traditional, on-premise software applications and locally hosted servers.

This whitepaper will examine the myths and realities of SaaS/Cloud Computing, the U.S.A. Patriot Act, and data privacy, with a focus on the CRM arena. We will also recommend reasonable approaches to overcome common corporate concerns so businesses can fully capitalize on the potential benefits of SaaS/Cloud Computing.

# Why Software-as-a-Service and Cloud Computing Are Gaining Corporate Attention and Adoption

Four macro-market trends are driving organizations of all sizes across nearly every industry to adopt SaaS and Cloud Computing solutions. These trends include:

- ***Changing economic conditions*** **–** The current financial crisis is forcing decision-makers to re-evaluate their capital investments and refocus their limited resources on their core competencies.
- ***Changing competitive forces*** **–** Globalization and eCommerce have opened new market opportunities, but also lowered the barriers to entry in nearly every industry, pressuring corporate margins and undercutting customer loyalty.
- ***Changing workplace requirements*** **–** The workplace is also being redefined by more dispersed and tech-savvy workers who are more mobile and adept at leveraging technology to perform their day-to-day jobs.
- ***Changing technology requirements*** **–** Broadband networks and powerful mobile devices are enabling employees to work anywhere. Flexible gird, blade and virtualization technologies, along with system automation and management capabilities are also making it easier to provision software and computing power.

Traditional, on-premise software applications and systems were not designed to respond to these trends and challenges. Instead, they were architected to address the needs of the more centralized organizations of the past. They have also proven to be too expensive and labor-intensive to deploy and maintain in today's tough economic environment.

It has become particularly challenging to secure corporate systems and software because it requires specialized skills and ongoing efforts. As a consequence, many on-premise applications and systems have failed to produce the return on investment (ROI) that organizations expected, and have required a higher total cost of ownership (TCO) to keep them up and running.

These trends are having a significant impact on markets where escalating competition is driving companies to seek more effective methods to meet the needs of their customers while properly supporting their employees and business partners.

The success of consumer-oriented 'on-demand' services has created a new set of expectations for how business applications should look and operate among corporate executives and end-users. THINKstrategies has seen a steady increase in customer interest and adoption of on-demand SaaS solutions driven by very high customer satisfaction rates which have led to over 90% renewal and referral rates.

Our research has been reinforced by a recent Gartner study which found that 95% of its survey respondents expected to maintain or grow their use of SaaS.[1] As a result of these positive customer reviews, IDC forecasts the SaaS market will experience a 25.3% compound annual growth rate (CAGR) and equal $40.5 billion by 2014.[2]

[1] "Gartner: SaaS Adoption on the Rise", NetworkWorld, May 5, 2010. http://www.networkworld.com/news/2010/050610-gartner-saas-adoption-on-the.html.
[2] "Worldwide Software as a Service 2010–2014 Forecast: Software Will Never Be the Same", IDC Report, June 2010, Doc # 223628.

SaaS-based CRM and customer service solutions, in particular, are seeing strong adoption. Today's business-to-consumer brands realize that delivering a consistent, satisfying customer experience across every customer touchpoint is critical to improving sales and customer loyalty. SaaS-based CRM solutions enable them to leverage the latest technologies to improve customer satisfaction and retention while minimizing the costs of on-premise CRM deployments and upgrades. As a result of these trends, leading market research firms predict that demand for SaaS or Cloud-based CRM solutions will exceed 25% a year through 2012, while traditional on-premise CRM system growth will only rise 10% over the same period.[3]

# Putting the U.S.A. Patriot Act in Proper Perspective

Despite the tangible business benefits being produced by today's SaaS and Cloud Computing solutions, many corporate decision-makers are still hesitant to acquire these services from U.S. providers because of the perceived threat posed by the U.S.A. Patriot Act.

The U.S.A. Patriot Act was instituted in 2001 in response to the 9/11 terrorist attacks. It contains strong language regarding the right of the American government to seek data regarding suspected individuals from corporate databases to counteract potential terrorist threats or other criminal activity.

While the powers outlined in this provision appear threatening, there are a number of reasons why corporate concerns about the U.S.A. Patriot Act have been overblown and should not get in the way of organizations fully leveraging today's powerful SaaS/Cloud Computing solutions.

### *Worldwide Anti-Terrorism Regulations Preclude Local Protections*

Although the U.S.A. Patriot Act gets most of the attention, the truth is that many countries have adopted similar provisions in the wake of rising terrorist threats and have also pledged cooperation across international borders.

For instance, the Canada Anti-Terrorism Act (ATA) was also introduced in October 2001, and includes many of the same stipulations as the U.S.A. Patriot Act. As a result, David Fraser, partner at Atlantic Canada-based law firm McInnes Cooper, has stated,

> *"The 'boogey man' of the U.S.A. Patriot Act has just become an easy excuse to say no [to Cloud Computing]…There's no absolute restriction or absolute privacy in Canada or in the U.S. when it comes to these sorts of things, so with that in mind, people need to make informed decisions about what they are going to do with their data."*[4]

This means that companies relying on local servers in Canada, or elsewhere, are equally at risk of government injunction as those organizations which leverage U.S.-based solutions, so there is no advantage in maintaining their own data locally.

[3] CRMforecast.com - On Demand CRM Software Research, Facts and Figures, http://www.crmforecast.com/saasresearch.htm
[4] "Don't Use the Patriot Act as an Excuse", Jennifer Kavur, ComputerWorld Canada, July 5, 2010. http://www.itworldcanada.com/ViewArticle.aspx?url=dont-use-the-patriot-act-as-an-excuse

### *Tough Policies Aimed at Real Terrorist and Other Criminal Elements, Not Legitimate Business Operations*

It is important to remember that the U.S.A. Patriot Act and similar regulations were designed to counteract terrorists and other international criminals.

These tough laws were not instituted to unilaterally gain access to legitimate corporate data or disrupt normal business operations.

Instead, the U.S.A. Patriot Act, ATA and similar regulations require law enforcement agencies to provide just cause for a court order to gain access to the personal records based on real terrorist or criminal threats.

The likelihood that governmental agencies will use this power to demand access to private data is very low and far outweighed by the real benefits of today's rapidly evolving Cloud Computing solutions.

### *Transborder Information Transmission Commonplace*

The Internet has made it easy for organizations and individuals to transmit and exchange information around the globe. The transfer of information across borders is referred to as *"transborder data flow".*

Although the Internet has accelerated this transborder data flow, companies and governments have been engaged in this type of activity for years directly through their own international operations, or as a part of an IT outsourcing (ITO) or business process outsourcing (BPO) arrangement which involves an international service provider.

Even everyday business operations can entail transborder data transfers. Whether it is simple email messages conveying sensitive data or more concerted data transfer as a part of enterprise application processing or other ongoing operations, moving data across international borders is a reality of day-to-day life.

### *No Cases of Inappropriate Private Data Requests Reported*

Fortunately, although these government regulations include tough legal terminology regarding the ability of government agencies to seek private data from corporations, there have not been any publicly reported cases in which any such request was deemed inappropriate by the parties involved.

Instead, government agencies have been highly selective in their use of this sensitive power in an effort to respect the privacy rights of individuals and organizations worldwide. As a result, there have not been any cases in which companies have publicly disputed government authorities which have sought private data as a part of an investigation.

Therefore, THINKstrategies believes that businesses should not allow their ill-placed concerns to get in the way of reaping the rewards of SaaS-based CRM systems.

Given the minimal threat actually created by the U.S.A. Patriot Act, ATA and similar government policies, THINKstrategies believes that it is more important to recognize the even greater data security threats which actually exist within today's corporate environment, and the added protection which the leading SaaS and Cloud Computing services offer to combat these threats.

# Recognizing the Real Security Threats in the Corporate World

The fact is that nearly every company, regardless of size, depends on the Internet to conduct business and compete in a global marketplace.

Therefore, organizations face a rapidly escalating array of security attacks on their sensitive corporate data every day. These threats come from increasingly skilled hackers trying to penetrate corporate databases from the outside, as well as the spiteful actions of disgruntled workers from the inside, or even the inadvertent mistakes of well-intentioned employees which could jeopardize critical data.

### *On-Premise Vulnerabilities Outpace On-Demand Threats*

The truth is that traditional on-premise systems with local client storage on company laptops are even more vulnerable to attack or other threats than cloud-based systems. There have been numerous stories of hackers accessing corporate credit card records supposedly protected behind company firewalls. And, employees often lose or have their company laptops stolen which house sensitive data.

For instance, T.J. Maxx reported in January, 2007, that hackers had accessed customer credit card and drivers license information creating concern for customers of T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico, Winners and Home Sense stores in Canada, as well as T.K. Maxx in the U.K. and Ireland.

Another example is the Heartland data breach of 2008 which also points to in-house security vulnerabilities. This Princeton, N.J.-based payments processor revealed that unknown intruders broke into its systems and planted malicious “sniffer” software designed to snag credit card numbers as they were transferred over the internal network. One of the largest payment processors in the country, it discovered the invasion only after receiving alerts from Visa and MasterCard.

### *Data Security Not a Core Competency for Most Corporations*

In today’s tough economic climate, it doesn’t make sense for companies to invest in greater security capabilities when they need to focus on their core businesses. No matter how great an investment an organization is willing to make in the latest security systems or specialized staff, few can hope to keep pace with the rising number of external threats and internal vulnerabilities.

Yet the reality is that many IT and business decision-makers remain concerned about losing control of their security capabilities by relying on a SaaS or Cloud Computing service provider to safeguard their data.

THINKstrategies believes that most organizations will actually benefit by leveraging the added security skills and resources which SaaS and Cloud Computing service providers have to offer.

# How SaaS & Cloud Computing Address Data Privacy Concerns

THINKstrategies has found that SaaS and Cloud Computing vendors, and the solutions they offer, can actually help organizations better protect their private data because these service providers are focused entirely on storing and processing mission-critical corporate data in a secure fashion.

### *Security is a Full-Time Job for SaaS and Cloud Computing Providers*

Because delivering reliable and secure services is essential to the success of SaaS and Cloud Computing providers, it is incumbent on them to invest heavily in best-in-class security systems, proven policies and procedures, as well as highly skilled personnel.

And, because most SaaS and Cloud Computing providers have to support a wide range of customers, they are obliged to institute security systems and policies which satisfy the most stringent and demanding of their customers.

In particular, SaaS and Cloud Computing CRM and Web Customer Experience Optimization solution providers have to take even greater precautions to secure their customers' sensitive data to ensure that this important information is properly protected.

The leading providers of SaaS-based CRM solutions have invested heavily in the latest sophisticated encryption, authentication, and access control and monitoring technologies, along with the skilled staff to administer these systems.

Leading SaaS companies use the most advanced technology for Internet security available today, including industry standard Secure Socket Layer (SSL) technology, server authentication and data encryption. These technologies ensure that customer data is inaccessible to unauthorized users and the customer's account activity is carefully monitored to identify any suspicious behavior. These SaaS companies also host their operations in a secure server environment that is firewall protected to prevent access by outside intruders.

### *Multi-Tenancy Enables Every Customer to Obtain the Highest Level of Data Protection on an Ongoing Basis*

The 'multi-tenant' architecture which underlies today's leading SaaS solutions and Cloud Computing services permits the service providers to deliver a uniform level of data protection to all of their customers.

The multi-tenant service delivery model also enables the providers to continuously roll out updates and enhancements to respond to the latest security threats to their entire customer base.

Using automated update procedures administered by certified personnel allows the service provider to address today's escalating security threats and data privacy requirements in a more thorough and effective fashion than most companies who are primarily focused on their core businesses.

## Summary & Recommendations

THINKstrategies believes companies of all sizes should capitalize on today's rapidly evolving SaaS and Cloud Computing alternatives to augment their in-house resources in order to more cost-effectively and quickly achieve their business objectives. SaaS-based CRM and other Cloud-oriented customer service tools are particularly important solutions in today's increasingly competitive marketplace, enabling businesses to exceed customer expectations while minimizing the cost of doing business online and across channels.

While today's tough anti-terrorist policies appear to open the door to possible governmental efforts to obtain private data from organizations using SaaS/Cloud solutions, history clearly shows that these risks are remote and far outweighed by the measurable business benefits which proven SaaS and Cloud Computing providers are already delivering.

In fact, we think corporate decision-makers will be pleased to learn how leading SaaS/Cloud providers are responding to escalating security threats and addressing customer concerns about government regulations, such as the U.S.A. Patriot Act.

Although we believe that safeguarding sensitive data from various threats is essential, there are far greater risks within many traditional, on-premise environments – whether within corporate data centers or locally hosted services – because they lack the skills and tools to maintain their security on an ongoing basis.

Therefore, THINKstrategies strongly recommends that IT and business decision-makers put aside these concerns and carefully evaluate the powerful new functional capabilities, as well as the security safeguards offered by leading SaaS and Cloud Computing providers.

### About THINKstrategies, Inc.

*THINKstrategies is the only strategic consulting services company formed specifically to address the unprecedented business challenges facing IT managers, solutions providers, and investors today as the technology industry shifts from a product-centric toward a services-driven business model. The company's mission is to help our clients re-THINK their corporate strategies, and refocus their limited resources to capitalize on today's rapidly evolving Cloud Computing, Software-as-a-Service and Managed Services to achieve their business objectives. THINKstrategies has also founded the* ***Software-as-a-Service Showplace*** *(www.saas-showplace.com), the largest and highest ranked vendor-independent, online directory and best practices resource center of SaaS solutions organized into 80 Application, Industry and Enabling Technology categories. The Showplace also includes information and insights regarding industry best practices. For more information regarding our unique services, visit www.thinkstrategies.com, or contact us at info@thinkstrategies.com.*