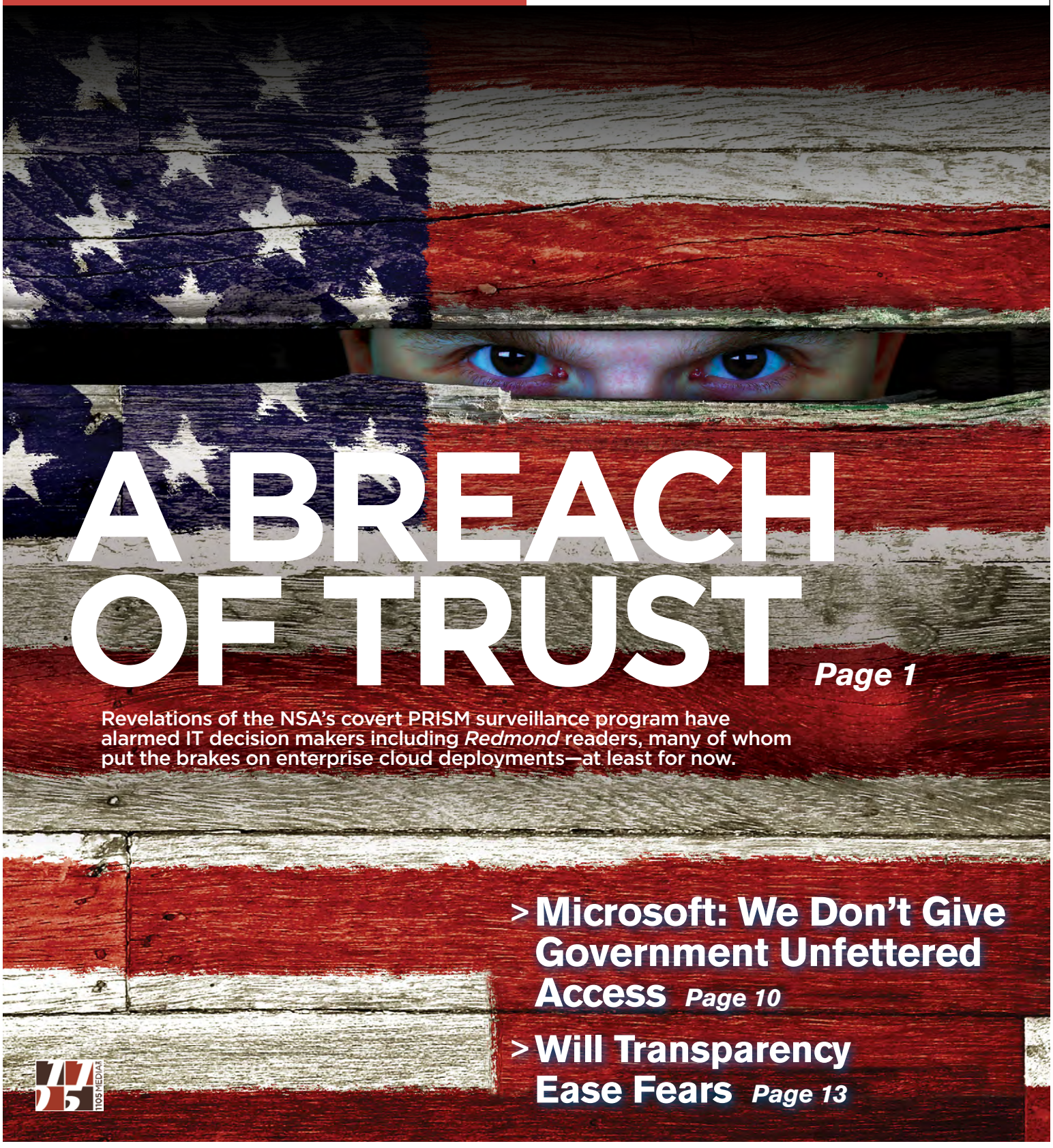
CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SPONSORED BY

GeoTrust®



A BREACH OF TRUST

Page 1

Revelations of the NSA's covert PRISM surveillance program have alarmed IT decision makers including *Redmond* readers, many of whom put the brakes on enterprise cloud deployments—at least for now.

> **Microsoft: We Don't Give Government Unfettered Access** *Page 10*

> **Will Transparency Ease Fears** *Page 13*

1105 MEDIA

A BREACH OF TRUST

Revelations of the NSA PRISM program and other surveillance operations have already put planned or existing use of public cloud services on ice. A survey of *Redmond* readers shows skepticism of the government and key providers–including Microsoft. BY CHRIS PAOLI

Revelations that the largest telecommunications and IT services providers have cooperated with the National Security Agency (NSA) to enable classified surveillance programs aimed at thwarting planned terrorist acts has had a chilling effect on cloud deployments. Since IT expert Edward Snowden brazenly leaked information about PRISM, the NSA's covert data collection and interception effort, a substantial number of businesses have either scaled back cloud initiatives or brought some deployments back in house.

As the nation debated whether Snowden was a whistleblower or a traitor, many organizations grappled with the prospect that their encrypted data might not be as secure as they believed it to be. For some, questions have been raised; for others, decisions are being second-guessed. While assessing whether their data could be accessed by the government or any third party without their knowledge or consent, businesses

have had to address the implications of that possibility and the newfound risks they face with their customers, regulators and shareholders.

According to the Information Technology and Innovation Foundation (ITIF), a Washington, D.C., think tank, cloud providers in North America alone stand to lose between $21.5 billion to $35 billion in revenues by 2016 following the disclosure that the NSA has secretly used stipulations of the Foreign Intelligence Surveillance Act (FISA) and the Patriot Act for programs such as PRISM to obtain and mine data to investigate suspected threats.

A survey of Redmond magazine's readership shows a significant number of organizations are putting some planned cloud migrations on hold.

If that sounds extreme, a survey of *Redmond* magazine's readership also shows a significant number of organizations are putting some planned cloud migrations on hold, while many are retreating from those already underway. More than one-third put planned projects on hold in wake of the NSA leaks, while 13 percent brought cloud projects back in-house, according to an online survey of 300 *Redmond* readers conducted in mid-August.

This was the mind set before last month's alarming revelation that the NSA allegedly has developed and used sophisticated techniques to decrypt encrypted data—sometimes with backdoor holes developed in concert with major players.

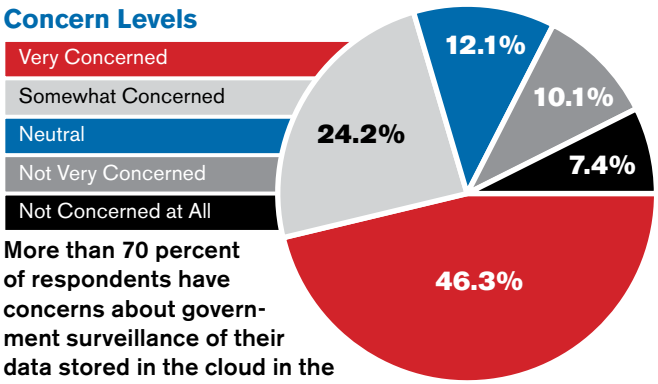
Temporary Panic?

While the data shows an overwhelming number of IT pros have new or heightened misgivings about the government and public cloud providers, those fears could subside in the coming months or years, some experts predict. That's especially the case as businesses realize they can use—or are already using—encryption and other security technologies that are impervious to surveillance.

Another factor that could ease fears is if the government becomes more transparent as to how and when data is retrieved—and lets providers do the same. Today providers complain they're hamstrung by the laws that prohibit such disclosures. Nevertheless, a sizable number of businesses have reacted to the disclosure of PRISM by voting with their budgets and retreating from existing and planned use of public cloud services.

The reason for this pullback is clear: Businesses are unnerved by the U.S. government's clandestine surveillance activities. Our survey shows 46 percent are "very concerned" and 24 percent are

Government Surveillance Concern Levels



More than 70 percent of respondents have concerns about government surveillance of their data stored in the cloud in the wake of the PRISM revelations. What long-term effect this has on cloud migrations remains to be seen.

"somewhat concerned" by the threat of the government accessing corporate data without consent.

As it pertains to IT security policies, more than half of respondents say addressing the threat of government surveillance of cloud data is a high priority, with 31.8 percent of that sample classifying it as a "very high" priority and 25 percent saying it's "somewhat high." Conversely, only 6.1 percent say addressing access of data by government officials is a "very low" priority, and 6.4 percent say the issue is "not a priority at all" to their IT shop.

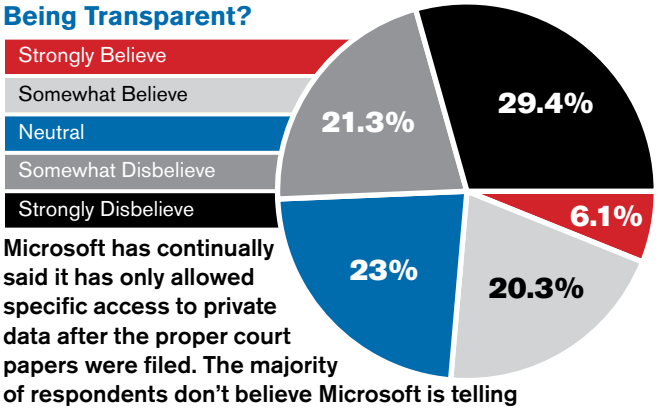
Unlike data-thieving criminals, government bodies have the techniques and legal avenues to get what they want, when they want it.

There are definitely valid reasons for the high levels of concern, according to Vikram Kumar, CEO of New Zealand-based cloud storage company Mega Ltd. Unlike data-thieving criminals, government bodies have the techniques and legal avenues to get what they want, when they want it, according to Kumar.

"Confidentiality and control over data have always been big concerns, in particular for corporate customers," Kumar says. "Concerns have probably increased recently. Government bodies typically have some tools that hackers don't–direct or internal system access, ability to issue gag orders, and 'full take' capabilities such as take everything."

All organizations should pause before putting sensitive data in public cloud services in the wake of the NSA leaks, says Travis C., a respondent to the *Redmond* survey. "This NSA issue has done an immense amount of harm in terms of trust for both the government and large data-housing companies," he says. "As the law is written, because you can't notify the client, we simply can't trust you. Microsoft and others need to allow clients to encrypt their own traffic with their own keys. The provider providing the encryption means nothing, as your key can be subpoenaed. If providers want to be trusted, they need to give the user control over his own encryption and make the government subpoena the subject of their investigation–as it should be."

Is Microsoft Being Transparent?



Microsoft has continually said it has only allowed specific access to private data after the proper court papers were filed. The majority of respondents don't believe Microsoft is telling the truth, while 20.3 percent somewhat believe that Microsoft is being transparent.

Microsoft's Alleged NSA Ties

While the disclosure of the covert surveillance activities identified a who's who of players–including Apple Inc., Google Inc., Facebook, Twitter, Verizon Communications Inc. and Yahoo! Inc.–Snowden alleged Microsoft in particular worked closely with the NSA to intercept communications from those using its key online services including SkyDrive, Office 365,

Outook.com and Skype. Indeed many of these services are targeted at consumers, but Office 365 includes hosted implementations of Exchange, SharePoint and Lync Online, and Microsoft's separate SkyDrive Pro is the service for storing SharePoint content.

In July, Snowden singled out Microsoft, claiming the company helped the NSA intercept communications by circumventing the service's own encryption. Microsoft adamantly denies it gave the NSA or any other entity backdoor access to its systems, saying it only grants government access to specific data requested through warrants, subpoenas or other legal channels.

Snowden singled out Microsoft, claiming the company helped the NSA intercept communications by circumventing the service's own encryption.

"There are significant inaccuracies in the interpretations of leaked government documents reported in the media," General Counsel Brad Smith said in a lengthy statement published days after the allegations regarding Microsoft's cooperation with the NSA (see "Microsoft: We Don't Give Government Unfettered Access," p. 10).

But a significant number of our survey respondents aren't so sure about that, with 29 percent saying they "strongly disbelieve" Microsoft's denial and 21.5 percent "somewhat" disbelieving the company's disavowal. Despite skepticism from half of our respondents, 5.8 percent "strongly believe" the company is telling the truth, while 20.5 percent "somewhat believe" the company's denial. The remaining 23.2 percent don't feel strongly either way.

While Microsoft says it supplies "customer data only when [Microsoft] receives a legally binding order or subpoena to do so, and never on a voluntary basis," according to Smith's response, what kind of data is actually being collected and shared?

What Data Is the Government Collecting?

Despite the National Security Agency (NSA) alleging it only collects metadata, the vast majority of readers don't believe that. More than 30 percent of readers believe specific, targeted communication data is being accessed, while more than half think the government is accessing everything being stored in the cloud.

Deployments to Microsoft Cloud Services Stalled

When former NSA contractor Edward Snowden alleged Microsoft was giving law enforcement agencies access to its datacenters (which the company denies), many are now reconsidering the use of Microsoft cloud services—and some even brought deployments back in-house.

More than half of the survey respondents (54.4 percent) believe Microsoft is providing the government access to "all personal and corporate data stored through Microsoft." Surprisingly, although the leaked allegations have pointed to cloud providers granting the NSA access to just metadata, only 10.1 percent believe this to be the case.

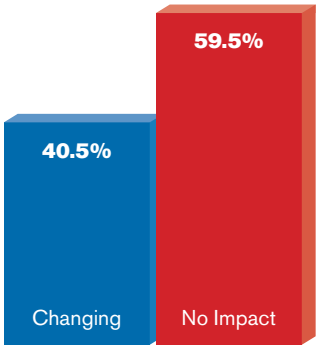
However, Microsoft isn't the only provider of which respondents are skeptical. Microsoft provides just as much data protection as other large cloud providers including Google, Amazon Web Services Inc. (AWS), Rackspace Inc. and IBM Corp., 60.2 percent of respondents say.

While it's understandable the disclosure of the NSA's surveillance activities has shaken IT decision makers' trust in cloud vendors, enterprises should be more concerned with the amount of transparency on the issue of data privacy coming from the federal government, says John Howie, chief operating officer of the Cloud Security Alliance (CSA), a non-profit consortium.

"Informed customers will likely understand that cloud providers are required by the laws of the countries in which they do business to reveal information to law enforcement when a valid warrant, court order or other legal document is produced, and that every cloud provider will respond only to lawful requests for access to data," Howie says. "There's likely more mistrust toward governments that request data than the cloud providers who are required to produce it. It's important to note that Microsoft, Google and others have asked governments worldwide for permission to publish some details about the requests made, such as the number and nature of requests, in order to be more transparent about the situation."

Impact of Cloud Budgets from NSA Leaks

Despite IT being concerned with using cloud services in the wake of the government surveillance allegations, a majority of respondents have not reacted by changing their budgets. In fact, 41.6 percent of those taking the poll say their spending will stay exactly the same, while 29.1 say it will actually be rising in the near future.



Planned Use of Microsoft Cloud Services in Wake of PRISM Revelations

While more than 20 percent see Microsoft's cloud offerings not able to provide adequate data protection compared to its competitors in the wake of the PRISM disclosures, almost 60 percent view all cloud vendors as equal.

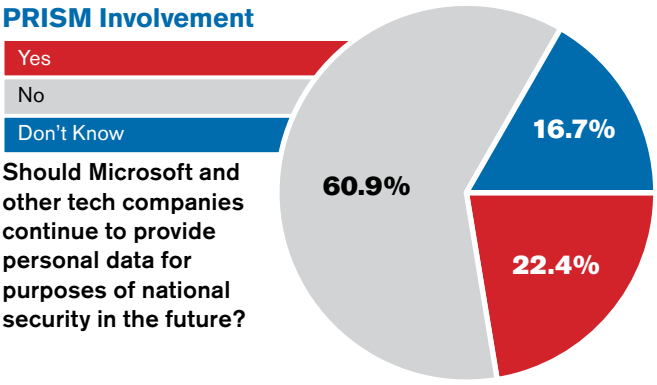
IT's Swift Reaction

Whether the mistrust lies at the feet of vendors or governments, the privacy implications have already had an impact on IT. One reader–who requested anonymity, given the sensitivity of the issue–says the government surveillance allegations have had a major impact on how his enterprise IT handles the cloud. "We don't have a whole lot of corporate data in the cloud. Thanks to PRISM we don't intend to place any more in the cloud, and will most likely remove what's already there," he explains.

Nearly half of those who responded to the survey appear to be reacting in a similar manner. When asked about current plans with regard to Microsoft cloud services, including Office 365, Outlook.com, Windows Azure and SkyDrive, 34.9 percent of respondents say their shop will "put some planned deployments on hold while assessing the situation." More alarming for the continual cloud growth trend is that 13.1 percent plan to bring cloud-stored data back in-house.

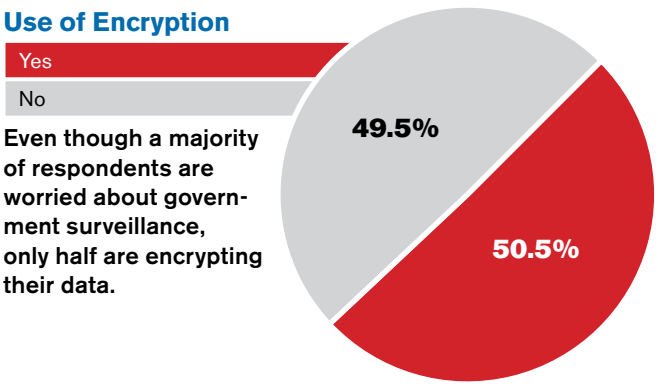
These findings also line up with a recent survey by the CSA, which found the information leaked by Snowden has led to 10 percent of non-U.S.-based participants canceling projects with U.S.-based companies like Microsoft, while 56 percent were less likely to use U.S.-based cloud providers.

Microsoft's Future PRISM Involvement



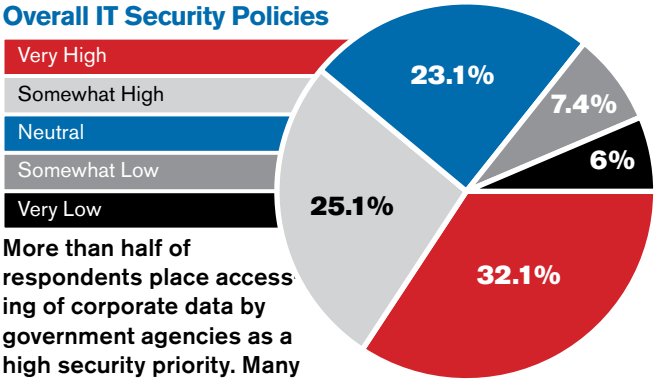
Should Microsoft and other tech companies continue to provide personal data for purposes of national security in the future?

Use of Encryption



Even though a majority of respondents are worried about government surveillance, only half are encrypting their data.

Government Surveillance Impact on Overall IT Security Policies



More than half of respondents place access ing of corporate data by government agencies as a high security priority. Many suggest that the risk to IT is just as high as traditional data breaches. While nearly one-quarter of respondents are ambivalent, few see it as a low priority.

For those willing to stick with Microsoft's cloud offerings, *Redmond* readers are divided on what actions to take. In an even split (50 percent), half say they're looking to increase encryption for data stored off-premises, while the other half will keep encryption levels the same.

This IT split on whether to increase encryption in the wake of PRISM clearly illustrates how many might be alarmed by the government's access to corporate cloud data–yet also shows many are unsure how to proceed. According to survey respondents, the answer includes encryption of some sort. Security solutions–including Microsoft BitLocker Drive Encryption, TrueCrypt, CipherPoint, the line of encryption services from Entrust Inc., and the third-party Mac encryption tool FileVault–were all given mentions by survey participants on what they're currently contemplating for improving their corporate data privacy.

And others who already have encryption enabled are double- checking their security in the wake of the PRISM revelations. "Our data is already encrypted. We're double-checking to ensure that traffic between our datacenter and off-site recovery site is adequately protected," commented one survey respondent.

While more than half of respondents are either "very concerned" or "somewhat concerned" to learn of government surveillance activities of their cloud-based data, it appears IT expenditures continue to flow through cloud providers. Even after the Snowden leaks, 42 percent of respondents to our survey say their cloud budgets will remain at current levels. And in some cases, cloud expenditures will continue to rise. Almost one-fifth of respondents (19.8 percent) say their budgets will experience a minor increase, and 9.2 percent say a major increase in spending is expected.

Gary McGraw, author and CTO of Cigital Inc., a Dulles, Va.-based consulting firm specializing in software security, says many IT organizations are struggling to determine how to act in wake of the PRISM disclosures, and the disclosures have created a sense of mistrust between customers and IT services providers.

"The real problem here is that all U.S. companies are playing by the same secret rules," McGraw says. "They haven't been telling their customers what's going on, because they're all expressly forbidden from doing so. Customers are obviously ticked off about this. And they no longer believe what their vendors are telling them—nor should they."

"Enterprises can definitely still use cloud applications and stay secure and compliant."

Paige Leidig, Senior VP, CipherCloud Inc.

The Encryption Key

So what can IT do when it comes to data privacy in the cloud? Should shops start pulling cloud-hosted corporate data back in-house, as 34.9 percent of respondents are doing?

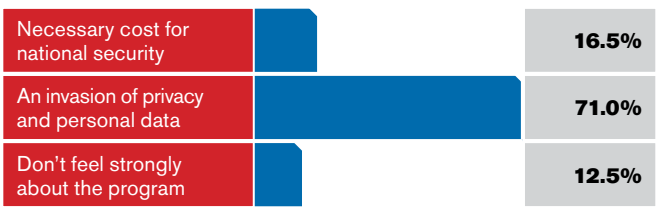
Users can still use cloud services from providers such as Microsoft and AWS as long as they're committed to encryption, says Paige Leidig, senior vice president of CipherCloud Inc., a cloud information protection firm based in San Jose, Calif.

"Enterprises can definitely still use cloud applications and stay secure and compliant," Leidig says. "The size of the provider actually doesn't affect the outcome. As the surveillance programs highlight, when it comes to protecting data on cloud applications, the best way is to go the ecosystem route. Users can layer additional protection controls on top of native security features from the cloud provider."

The layers added include encryption that covers your data at rest, in transit and in use, according to the CSA's recommended cloud best practices. This three-pronged approach ensures data is secured every step of the way.

Until recently, IT management has remained lax about covering the bases on all three fronts. But businesses are finally

The Cost of PRISM



An overwhelming majority of respondents view PRISM as an invasion of privacy.

catching on that encryption of data at rest and in transit isn't adequate–encrypting data in use "is critical," says Elad Yoran, chairman and CEO of Vaultive, a New York-based data encryption firm focused on cloud security. "If one fails to encrypt data in use, it's like leaving the front door or window wide open," he says.

Microsoft has already stated that it's obligated to provide data to federal law enforcement agencies with the proper court orders. If the data sought can also be decrypted from the providers, end users could have no idea when law enforcement is targeting their data. Yoran warns that having these providers hold onto the keys takes the issue of data ownership out of the hands of the enterprise. "The rule with encryption is whoever controls the keys controls the data," he says.

While Microsoft doesn't require users to hand over encryption keys when using its line of cloud-based services, Yoran says this might not be true for all providers–and those that do require holding onto the keys should be avoided.

Overall, readers participating in the Redmond survey don't view the PRISM surveillance program as a necessary cost for national security.

Privacy Trumps National Security

Overall, readers participating in the *Redmond* survey don't view the PRISM surveillance program as a necessary cost for national security–71 percent say it's "an invasion of privacy and personal data." When asked why it was looked upon so unfavorably, the No. 1 answer was the lack of trust due to the culmination of misinformation and secrecy on the parts of both cloud providers and government bodies.

As the NSA leaks have dominated both the national and technology dialog over the past several months, President Barack Obama in August proposed allowing law enforcement agencies and services providers to become more transparent about government surveillance programs. However, without specifics on when and how this would work–and whether President Obama could win congressional approval to enable such changes–the secretive surveillance of cloud data looks to be a trend that will continue. And it's a trend not unique to the United States.

"It's important to note that the U.S. government is not the only government in the world that can and will make requests of cloud providers for data," says CSA's Howie. "The United Kingdom, for example, has very similar legislation to the Patriot Act, and with respect to the collection of communications metadata it should be understood that the European Union passed the Data Retention Directive [in 2006], which goes much further than the U.S. government appears to."

While a three-pronged encryption strategy with control over the keys will help to increase the amount of disclosure end users receive

when their cloud-based data is accessed, it's up to those in IT to continue to keep the conversation about transparency and data ownership rights in the national discussion.

Fears Overblown?

Forrester Research Inc., pointing to the ITIF forecast that PRISM could cost cloud providers up to $35 billion by 2016, modeled a worst-case scenario where the true cost of PRISM to cloud services providers could total $180 billion, or 25 percent of overall IT services provider revenues, by that time frame.

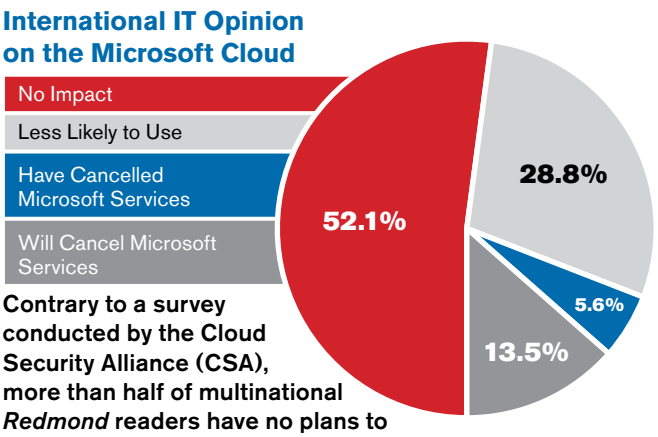
Forrester Research Inc. modeled a worst-case scenario where the true cost of PRISM to cloud services providers could total $180 billion by 2016.

Nevertheless, Forrester cloud computing analyst James Staten said in a mid-August blog post that, while this doomsday picture is possible, it'll only materialize if the mindset of people and business decision makers persists over the next three years—a likelihood he sees as remote.

"Prior to today's media-hyped paranoia about government surveillance, corporate IT spending has been trending toward outsourcing for many years," Staten noted. "Few corporations have no data in the cloud, let alone no data with a hosting company, co-location provider or outsourcing firm."

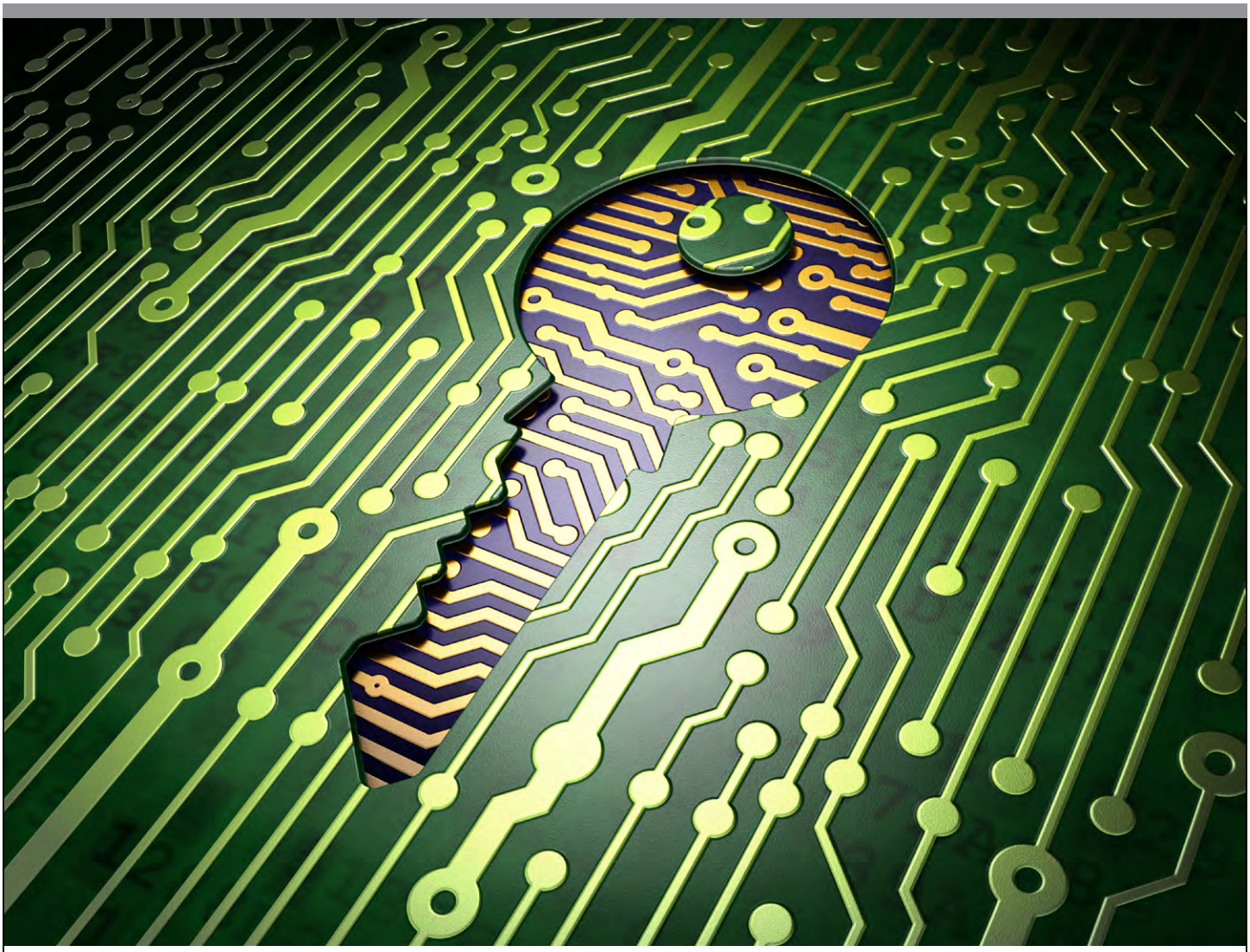
And Staten doesn't see that changing over the long term, as business realities—both economic and practical—will necessitate the use of public cloud infrastructure and Software as a Service (SaaS) in order for businesses to deliver IT.

"The fact of the matter is that the IT services market is a part of our portfolios because it provides capabilities we value either against IT or business metrics," Staten noted. "And it's highly likely these values are worth more to you than the potential risk you think your company faces due to government surveillance. If your company is a prime target for government surveillance, you're probably being watched from within your own firewalls right now." R



Contrary to a survey conducted by the Cloud Security Alliance (CSA), more than half of multinational *Redmond* readers have no plans to change their usage of Microsoft cloud services. However, more than one-quarter are less likely to use the company's services after the PRISM leaks, and 13.5 percent are considering dropping all Microsoft cloud services.

Chris Paoli is associate Web editor for the 1105 Enterprise Computing Group. Redmond *Editor Jeffrey Schwartz contributed reporting to this article.*



Microsoft: We Don't Give Government Unfettered Access

Among many of the classified surveillance activities leaked by Edward Snowden was that Microsoft was giving the National Security Agency (NSA) access to the systems that run services such as SkyDrive, Skype, Office 365 and Outlook.com (formerly Hotmail).

Snowden was an employee and IT expert at NSA contractor Booz Allen Hamilton Inc. with broad access to classified information. Booz Allen immediately terminated his employment

Brad Smith

when he revealed himself as the leaker of the surveillance activities. Snowden had also worked for other IT contractors in the past.

In response to Snowden's charge about Microsoft's activities, the company's General Counsel Brad Smith denied that it was giving such access. While Smith said the company was limited by law in what it can say and called on the Attorney General to ease those restrictions, he did offer what he was permitted to disclose. Here's an edited summary (the full response can be accessed online at **bit.ly/12Hs1KC**):

- **Enterprise E-mail and Document Storage:** If we receive a government demand for data held by a business customer, we take steps to redirect the government to the customer directly, and we notify the customer unless we are legally prohibited from doing so. We have never provided any government with customer data from any of our business or government customers for national security purposes. In terms of criminal law enforcement requests, we made clear in our Law Enforcement Requests Report that throughout 2012 we only complied with four requests related to business or government customers. In three instances, we notified the customer of the demand and they asked us to produce the data. In the fourth case, the customer received the demand directly and asked Microsoft to produce the data. We do not provide any government with the ability to break the encryption used between our business customers and their data in the cloud, nor do we provide the government with the encryption keys.
- **Outlook.com** (formerly Hotmail): We do not provide any government with direct access to e-mails or instant messages. Like all providers of communications services, we are sometimes obligated to comply with lawful demands from governments to turn over content for specific accounts, pursuant to a search warrant or court order. This is true in the United States and other countries where we store data. When we receive such a demand, we review it and, if obligated to, we comply. Cutting through the technical details, all of the information in the recent leaked government documents adds up to two things. First, while we did discuss legal compliance requirements with the government as reported, in none of these discussions did Microsoft provide or agree to provide any government with direct access to user content or the ability to break our encryption. Second, these discussions were instead about how Microsoft would meet its continuing obligation to comply with

"If we receive a government demand for data held by a business customer, we take steps to redirect the government to the customer directly."

–Brad Smith, Microsoft general counsel

"We will not provide governments with direct or unfettered access to customer data or encryption keys."

–Brad Smith, Microsoft general counsel

the law by providing specific information in response to lawful government orders.

- **SkyDrive:** We respond to legal government demands for data stored in SkyDrive in the same way. In 2013 we made changes to our processes to be able to continue to comply with an increasing number of legal demands of governments worldwide. None of these changes provided any government with direct access to SkyDrive. The process used for producing SkyDrive files is the same whether it is for a criminal search warrant or in response to a national security order, in the United States or elsewhere.
- **Skype Calls:** We continue to enhance and evolve the Skype offerings and have made a number of improvements to the technical back-end for Skype, such as the 2012 move to in-house hosting of "supernodes" and the migration of much Skype IM traffic to servers in our datacenters. These changes were not made to facilitate greater government access to audio, video, messaging or other customer data. Looking forward, as Internet-based voice and video communications increase, it is clear that governments will have an interest in using (or establishing) legal powers to secure access to this kind of content to investigate crimes or tackle terrorism. We therefore assume that all calls, whether over the Internet or by fixed line or mobile phone, will offer similar levels of privacy and security. We will not provide governments with direct or unfettered access to customer data or encryption keys. R

Will Transparency Ease Fears?

BY JEFFREY SCHWARTZ

As the disclosure of PRISM and other data surveillance activities by the U.S. government threatens the use of the cloud, Microsoft and other telecommunications, Internet and IT services providers are calling on the government to let them be more transparent with their customers.

Immediately after Edward Snowden claimed Microsoft was letting the National Security Agency (NSA) directly access data from its various services, a charge the company denies, Microsoft General Counsel Brad Smith asked Attorney General Eric Holder to let the company "share publicly more complete information about how we handle national security requests for customer information. We hope the Attorney General can step in to change this situation."

This is a pressing issue for all cloud providers as they seek to assure business customers and consumers alike that they're protecting their data.

This is a pressing issue for all cloud providers as they seek to assure business customers and consumers alike that they're protecting their data. In August, the Cloud Security Alliance (CSA) held an online roundtable whose participants agreed on the need for improved transparency. "Today, there's no mechanism in place for cloud customers, or any user organizations that rely on these cloud providers, to know when their data was exposed," said event moderator Elad Yoran, VP of finance with the New York City chapter of the CSA and the CEO of Vaultive, a provider of a cloud encryption service.

"This is definitely a hot topic for me," added panelist Peter McGoff, general counsel of Box, the popular cloud storage provider. "One thing we look at as a cloud provider, and what we're asking for, is more transparency in the process. We want to be able to communicate to customers at a minimum the numbers of such requests that we get in and what our process is. Right now, it's not quite clear that we have that flexibility."

McGoff did offer that Box hasn't received an overwhelming number of warrants for enterprise data. Until early August, the Obama administration had resisted supporting changes in the disclosure policies, but the President proposed the government step up its efforts to be transparent. How that proposal plays out remains to be seen, but McGoff sees it as a move in the right direction.

"It's a good first step," he said. "I felt much better with President Obama coming out and putting a bright light on this." Also on the CSA webcast was Robert Brammer, a senior advisor to the Internet2 consortium and CEO of Brammer Technology LLC, who agreed. "The review the President has talked about, with the intelligence process [and] with one of the objectives to create more transparency, will improve the level of dialogue on this subject," he said.

The Obama administration also released a white paper (available at **bit.ly/15ZprFx**) that lays out how telecommunications providers access and analyze metadata gathered from calling information.

"This information is limited to telephony metadata, which includes information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted," according to the white paper's executive summary. "Importantly, this information does not include any information about the content of those calls–the government cannot, through this program, listen to or record any telephone conversations."

While that may be true, there are plenty of skeptics. Only 10.1 percent of those surveyed by ***Redmond*** magazine believe the

government is only accessing metadata. While Snowden revealed surveillance efforts that were previously not public, much of the concern that has surfaced is old news, added Francoise Gilbert, founder and managing director of IT Law Group, a law firm focused on domestic and international information privacy and security.

During the CSA roundtable panel discussion, Gilbert pointed out the U.S. government has had surveillance initiatives in place dating back to the late 1960s, and the Foreign Intelligence Surveillance Act (FISA) was initiated in 1978.

The U.S. government has had surveillance initiatives in place dating back to the late 1960s, and the Foreign Intelligence Surveillance Act (FISA) was initiated in 1978.

"The topic of government access to data is not something new," she said. "There have been many iterations and many amendments to these laws to keep up with technology and technology progress, and there has been a movement for the past two years to amend one of these laws–the Electronic Communications Privacy Act–to also bring it to the 21st century."

Gilbert also pointed to due-process requirements such as the Wiretap Act. While critics of the Foreign Intelligence Surveillance Court (FISC), created under FISA, believe the judges rubber-stamp most law enforcement warrants, Gilbert argued that United States citizens have more protections than those in many foreign countries, such as the United Kingdom.

"There is no FISA court–they just come in and have access to your information," she said of many foreign counties. "In general, I'd say the laws are definitely more favorable to the governments in foreign countries, especially in the United Kingdom," as compared to the United States, she explained.

This may be true, but there's a growing chorus of critics in the United States who don't view the current laws–including the Patriot Act–as very favorable to their privacy. While the government argues its surveillance efforts have thwarted potentially deadly attacks, 71 percent of respondents to the ***Redmond*** survey don't view surveillance efforts such as the PRISM program as a necessary cost of national security. The panelists during the CSA webcast concurred that the feds are going to have to look at becoming more transparent. R

Jeffrey Schwartz is editor of Redmond.