ITIF
The Information Technology & Innovation Foundation

How Much Will PRISM Cost the U.S. Cloud Computing Industry?

BY DANIEL CASTRO | AUGUST 2013

The U.S. cloud computing industry stands to lose $22 to $35 billion over the next three years as a result of the recent revelations about the NSA's electronic surveillance programs.

The recent revelations about the extent to which the National Security Agency (NSA) and other U.S. law enforcement and national security agencies have used provisions in the Foreign Intelligence Surveillance Act (FISA) and USA PATRIOT Act to obtain electronic data from third-parties will likely have an immediate and lasting impact on the competitiveness of the U.S. cloud computing industry if foreign customers decide the risks of storing data with a U.S. company outweigh the benefits.

The United States has been the leader in providing cloud computing services not just domestically, but also abroad where it dominates every segment of the market. In the 2013 Informa Cloud World Global Insights survey, 71 percent of respondents (of which only 9 percent were from North America) ranked the United States as the leader in cloud computing usage and innovation.[1] In this same survey, nine out of ten respondents linked cloud computing to their country's economic competitiveness.

But other countries are trying to play catch-up to the United States' early success. Of the $13.5 billion in investments that cloud computing service providers made in 2011, $5.6 billion came from companies outside North America.[2] Even national governments are helping to bankroll these efforts to combat U.S. market leadership—France, for example, invested €135 million in a joint venture in cloud computing.[3]

At stake is a significant amount of revenue. As shown in figure 1, the global enterprise public cloud computing market will be a $207 billion industry by 2016.[4] Europeans in particular are trying to edge out their American competitors, and they are enlisting their

governments to help. Jean-Francois Audenard, the cloud security advisor to France Telecom, said with no small amount of nationalistic hyperbole, "It's extremely important to have the governments of Europe take care of this issue because if all the data of enterprises were going to be under the control of the U.S., it's not really good for the future of the European people."[5]

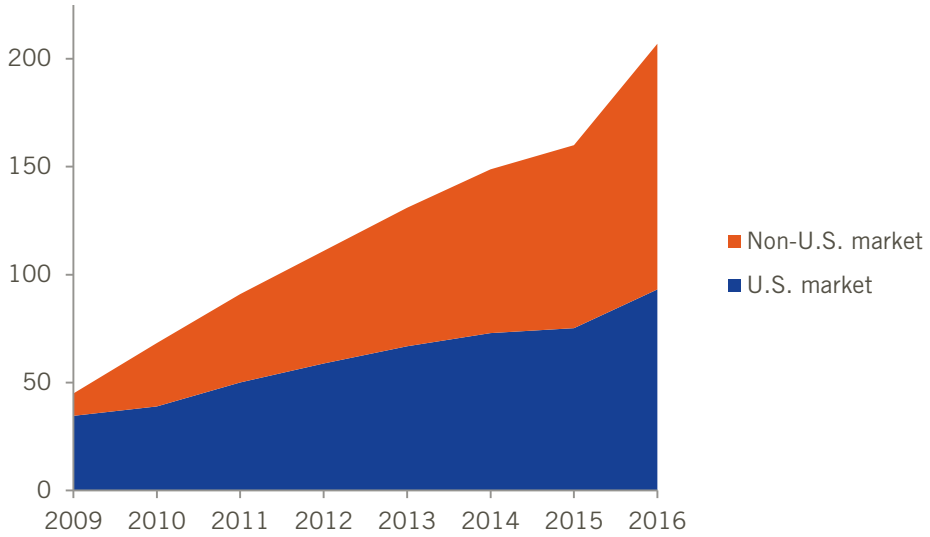

Figure 1: Worldwide spending on cloud computing for U.S. and non-U.S. markets, 2009 – 2016, $ billions.[6]

And governments have begun to respond. In a 2012 policy document titled "Unleashing the Potential of Cloud Computing in Europe," the European Commission (EC) called for a number of steps to promote cloud computing adoption in Europe, including creating pan-European technical standards, EU-wide certification for cloud computing providers, and model contract language.[7] The Europeans are quite frank about their intentions. The EC notes "this strategy is about building a new industry, and better competing against the United States in particular."[8] Gartner estimates that in Western Europe alone the cloud computing market will be $47 billion by 2015, and the EC estimates that European cloud computing providers stand to gain €80 billion in revenue by 2020.[9]

While much of this projected growth was until recently up for grabs by U.S. companies, the disclosures of the NSA's electronic surveillance may fundamentally alter the market dynamics. Neelie Kroes, European Commissioner for Digital Affairs, stated the problem quite succinctly, "If European cloud customers cannot trust the United States government, then maybe they won't trust U.S. cloud providers either. If I am right, there are multibillion-euro consequences for American companies. If I were an American cloud provider, I would be quite frustrated with my government right now."[10]

The impact of PRISM on U.S companies may be particularly acute because cloud computing is a rapidly growing industry. This means that cloud computing vendors not only have to retain existing customers, they must actively recruit new customers to retain

market share. Global spending on cloud computing is expected to grow by as much as 100 percent between 2012 and 2016, whereas the global IT market will only grow by 3 percent.[11] If U.S. companies lose market share in the short term, this will have long-term implications on their competitive advantage in this new industry.

Rival countries have noted this opportunity and will try to exploit it. One tactic they used before the PRISM disclosures was to stoke fear and uncertainty about the USA PATRIOT Act to argue that European businesses should store data locally to protect domestic data from the U.S. government.[12] Reinhard Clemens, CEO of Deutsche Telekom's T-systems group, argued in 2011 that creating a German or European cloud computing certification could advantage domestic cloud computing providers. He stated, "The Americans say that no matter what happens I'll release the data to the government if I'm forced to do so, from anywhere in the world. Certain German companies don't want others to access their systems. That's why we're well-positioned if we can say we're a European provider in a European legal sphere and no American can get to them."[13] And after the recent PRISM leaks, German Interior Minister Hans-Peter Friedrich declared publicly, "whoever fears their communication is being intercepted in any way should use services that don't go through American servers."[14] Similarly, Jörg-Uwe Hahn, a German Justice Minister, called for a boycott of U.S. companies.[15] After PRISM, the case for national clouds or other protectionist measures is even easier to make.

FINDINGS: THE IMPACT ON U.S. CLOUD SERVICE PROVIDERS

Just how much do U.S. cloud computing providers stand to lose from PRISM? At this stage it is unclear how much damage will be done, in part because it is still not certain how the U.S. government will respond. But it is possible to make some reasonable estimates about the potential impact.

On the low end, U.S. cloud computing providers might lose $21.5 billion over the next three years. This estimate assumes the U.S. eventually loses about 10 percent of foreign market to European or Asian competitors and retains its currently projected market share for the domestic market.

On the high end, U.S. cloud computing providers might lose $35.0 billion by 2016. This assumes the U.S. eventually loses 20 percent of the foreign market to competitors and retains its current domestic market share. (See Appendix A for details.)

What is the basis for these assumptions? The data are still thin—clearly this is a developing story and perceptions will likely evolve—but in June and July of 2013, the Cloud Security Alliance surveyed its members, who are industry practitioners, companies, and other cloud computing stakeholders, about their reactions to the NSA leaks.[16] For non-U.S. residents, 10 percent of respondents indicated that they had cancelled a project with a U.S.-based cloud computing provider; 56 percent said that they would be less likely to use a U.S.-based cloud computing service. For U.S. residents, slightly more than a third (36 percent) indicated that the NSA leaks made it more difficult for them to do business outside of the United States.

Thus we might reasonably conclude that given current conditions U.S. cloud service providers stand to lose somewhere between 10 and 20 percent of the foreign market in the next few years. Indeed, some foreign providers are already reporting their success. Artmotion, Switzerland's largest hosting company, reported a 45 percent increase in revenue in the month after Edward Snowden revealed details of the NSA's PRISM program.[17] And the percentage lost to foreign competitors could go higher if foreign governments enact protectionist trade barriers that effectively cut out U.S. providers. Already the German data protection authorities have called for suspending all data transfers to U.S. companies under the U.S.-EU Safe Harbor program because of PRISM.[18]

While the reputations of U.S. cloud computing providers (even those not involved with PRISM) are unfortunately the ones being most tarnished by the NSA leaks, the reality is that most developed countries have mutual legal assistance treaties (MLATs) which allow them to access data from third parties whether or not the data is stored domestically.[19] The market research firm IDC noted in 2012, "The PATRIOT Act is nothing special, indeed data stored in the US is generally better protected than in most European countries, in particular the UK."[20] In Germany (yes, the same country that wants to suspend data transfers to the United States) the G10 act gives German intelligence officials the ability to monitor telecommunications without a court order.[21]

RECOMMENDATIONS

So what should the U.S. government do?

First, U.S. government needs to proactively set the record straight about what information it does and does not have access to and how this level of access compares to other countries. To do this effectively, it needs to continue to declassify information about the PRISM program and allow companies to reveal more details about what information has been requested of them by the government. The economic consequences of national security decisions should be part of the debate, and this cannot happen until more details about PRISM have been revealed.

Second, the U.S. government should work to establish international transparency requirements so that it is clear what information U.S.-based and non-U.S.-based companies are disclosing to both domestic and foreign governments. For example, U.S. trade negotiators should work to include transparency requirements in trade agreements, including the Transatlantic Trade and Investment Partnership (TTIP) currently being negotiated with the EU.

Taking these steps will help ensure that national security interests are balanced against economic interests, and that U.S. cloud service providers are able to effectively compete globally.[22]

CONCLUSION

The United States has both the most to gain and the most to lose. Many of the economic benefits of cloud computing, such as job growth and revenue, are dependent on the United States being able to export cloud computing services. If U.S. firms are to maintain their

lead in the market, they must be able to compete in the global market. It is clear that if the U.S. government continues to impede U.S. cloud computing providers, other nations are more than willing to step in to grow their own industries at the expense of U.S. businesses.

APPENDIX A: DETAILED ESTIMATES

The details of the data and assumptions used to calculate these estimates are provided below. See the text and related endnotes for further explanation and sources.

Low Estimate

	2014	2015	2016
Global market	$148.8	$160.0	$207.0
U.S. market	$72.9	$75.2	$93.2
Non-U.S. market	$75.9	$84.8	$113.9
U.S. share of non-U.S. market (Pre-PRISM)	85%	80%	75%
U.S. share of non-U.S. market (Post-PRISM)	80%	73%	65%
U.S. revenue from non-U.S. (Pre-PRISM)	$64.5	$67.8	$85.4
U.S. revenue from non-U.S. market (Post-PRISM)	$60.7	$61.5	$74.0
Annual loss	$3.8	$6.4	$11.4
Total three-year loss	$21.5		

Table 1: Low estimate of losses from NSA revelations, in $ billions.

High Estimate

	2014	2015	2016
Global market	$148.8	$160.0	$207.0
U.S. market	$72.9	$75.2	$93.2
Non-U.S. market	$75.9	$84.8	$113.9
U.S. share of non-U.S. market (Pre-PRISM)	85%	80%	75%
U.S. share of non-U.S. market (Post-PRISM)	80%	70%	55%
U.S. revenue from non-U.S. (Pre-PRISM)	$64.5	$67.8	$85.4
U.S. revenue from non-U.S. market (Post-PRISM)	$60.7	$59.4	$62.6
Annual loss	$3.8	$8.5	$22.8
Total three-year loss	**$35.0**		

Table 2: High estimate of losses from NSA revelations, in $ billions.

ENDNOTES

1. Camille Mendler, "2013 Informa Cloud World Global Insights," Informa Telecoms and Media (2013), http://www.informatandm.com/cloud-monitor/.
2. Camille Mendler, "Navigating the Telecom Cloud: Growth Perspectives," Informa Telecoms and Media (2013), http://www.informatandm.com/wp-content/uploads/2012/05/Informa-Telecom-Cloud-white-paper.pdf.
3. "France to form Andromede cloud computing JV in November," Telecom.paper, 2011, http://www.telecompaper.com/news/france-to-form-andromede-cloud-computing-jv-in-november--828913.
4. "Gartner Predict Cloud Computing Spending to Increase by 100% in 2016, Says AppsCare," PRWeb.com, 2012, http://www.prweb.com/releases/2012/7/prweb9711167.htm.
5. Cornelius Rahn, "Europe Won't Let U.S. Dominate Cloud With Rules to Curb HP: Tech," Bloomberg, January 17, 2012, http://www.bloomberg.com/news/2012-01-17/europe-won-t-let-u-s-dominate-cloud-with-rules-to-curb-hp-tech.html.
6. Spending estimates based on publicly reported data from Gartner including "Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010," Gartner, 2010, http://www.gartner.com/newsroom/id/1389313, "Gartner Says Worldwide IT Spending On Pace to Surpass $3.6 Trillion in 2012," Gartner, 2012, http://www.gartner.com/newsroom/id/2074815, "Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion," Gartner, 2013, http://www.gartner.com/newsroom/id/2352816, Andrew Hickey, "Cloud Computing Services Market To Near $150 Billion In 2014," CRN, 2010, http://www.crn.com/news/channel-programs/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm, and "Global public cloud services market to exceed $180 billion by 2015: Gartner," The Hindu, 2013, http://www.thehindu.com/sci-tech/technology/internet/global-public-cloud-services-market-to-exceed-180-billion-by-2015-gartner/article4966812.ece. U.S. versus non-U.S. market share based on data from "Market overview & forecast." Telecom and IT Market Research Report. MarketsandMarkets, 2010. 14+. Business Insights: Global. Web. 23 July 2013.
7. "Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me?" European Commission, 2012, http://europa.eu/rapid/press-release_MEMO-12-713_en.htm.
8. Ibid.
9. Rahn, "Europe Won't Les U.S. Dominate Cloud."
10. Ian Traynor, "European firms 'could quit US internet providers over NSA scandal,'" The Guardian, July 4, 2013, http://www.theguardian.com/world/2013/jul/04/european-us-internet-providers-nsa.
11. "Gartner Predict Cloud Computing Spending to Increase by 100% in 2016, Says AppsCare," PRWeb.com.
12. Zack Whittaker, "Defense giant ditches Microsoft's cloud citing Patriot Act fears," ZDNet.com, December 2011, http://www.zdnet.com/blog/london/defense-giant-ditches-microsofts-cloud-citing-patriot-act-fears/1349.
13. Cornelius Rahn, "Deutsche Telekom Wants `German Cloud' to Shield Data From U.S." Bloomberg, September 13, 2011, http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html.
14. "German minister: drop Google if you fear US spying," Associated Press, July 3, 2012, http://news.yahoo.com/german-minister-drop-google-fear-us-spying-105524847.html.
15. Georgina, Prodhan and Claire Davenport, "US surveillance revelations deepen European fears," Reuters, June 7, 2013, http://www.reuters.com/article/2013/06/07/europe-surveillance-prism-idUSL5N0EJ31S20130607.
16. "CSA Survey Results: Government Access to Information," Cloud Security Alliance, July 2013, https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf.
17. David Giilbert, "Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations," International Business Times, July 4, 2013, http://au.ibtimes.com/articles/486613/20130704/business-turns-away-dropbox-towards-switzerland-nsa.htm.

18. Jabeen Bhatti, "In Wake of PRISM, German DPAs Threaten To Halt Data Transfers to Non-EU Countries," Bloomberg BNA, July 29, 2013, http://www.bna.com/wake-prism-german-n17179875502/.
19. Winston Maxwell and Christopher Wolf, "A Global Reality: Government Access to Data in the Cloud," Hogan Lovells, July 18, 2012, http://m.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised Government Access to Cloud Data Paper (18 July 12).pdf.
20. "Patriot Act not a cloud computing threat: IDC," Continuity Briefing, October 2012, http://www.continuitycentral.com/news06514.html.
21. Maxwell and Wolf, "A Global Reality."
22. See also, Daniel Castro, "Digital trade in a post-PRISM world," The Hill, July 24, 2013, http://thehill.com/blogs/congress-blog/technology/312887-digital-trade-in-a-post-prism-world.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing input to this report: Rob Atkinson and Will Dube. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation and Director of the Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION VISIT WWW.ITIF.ORG.