A Transformative Era in Cloud Computing: Questions, Developments, and Affirmations in Light of Snowden's NSA Revelations

Cloud computing has been single-handedly impacted and brought into a new era by Edward Snowden's National Security Agency (NSA) revelations in June 2013. The watershed year of 2013 has been described as "an inflection point,"[1] a complete shift in direction in the Internet, in which "the curtain (was) raised on the surveillance state."[2] The resultant public alarm regarding NSA Internet surveillance is particularly relevant in cloud computing, where data is housed and managed by external organizations. This 2013 seismic shift coincides with the first annual report by the Internet Monitor research project of the Berkman Center for Internet & Society at Harvard University, entitled "Internet Monitor 2013: Reflections on the Digital World." This report and the flurry of news articles addressing Snowden's NSA revelations present a multi-faceted microcosm through which to examine the impact of Snowden's revelations on the double-edged sword of international cloud computing. Cloud computing's ongoing controversy— its benefits of cost efficiency and flexibility versus its risk of privacy issues— now has been brought to new heights by Snowden's revelations of NSA surveillance. The Snowden revelations' upside is that public awareness has been illuminated and concern for individual rights has been rekindled, while its downside is that American cloud computing's explosive global growth and dominance has been called into question. Policy must be recalibrated to honor public and private rights equally for a healthy

balance between national security and individual security, in order to preserve American dominance in cloud computing.

First, I will discuss the state of affairs preceding Snowden's NSA Revelations in May 2013. Then, I will show effect—the impact on cloud computing. Finally, I will discuss the future—implications and suggestions—to lead toward a convergent cooperative balance between individual security and national security in cloud computing.

1. The State of Affairs Before Snowden's NSA Revelations

1.1 Cloud Computing Overview:

Cloud computing refers to the storage of data in external networks, rather than in users' local computers, generally through the Internet.[3] Due to cost and flexibility benefits, the explosive trend toward the use of cloud computing's off-site data storage has been rapidly replacing the dominance of traditional in-house Information Technology (IT). Cloud computing's three levels— Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)— are interconnected. SaaS is the top most easily recognized form of the cloud with which the consumer interacts directly, PaaS is the middle portion that acts as framework for hosting and developing programs and application, and IaaS is the large foundational infrastructure of power, physical servers, and storage.[4]

Software as a Service (SaaS):

SaaS provides software for the end user remotely through the Internet or an alternate network. Examples of SaaS include Gmail, Google and Facebook. The "hegemony of these giants"[5] represent just one evolutionary development in the so-far "Three Generations of the Networked Public Sphere," or NPS, according to author John Kelly. The first generation was only five or six years ago in the form of decentralized blogospheres. The second generation occurred with the all-powerful influence of new social media giants like Facebook and Twitter. The currently evolving third generation of the NPS is the addition of social media platforms like Tumblr and Pinterest that supplement, rather than supplant, the towering giants of Facebook and Twitter. Kelly likens the social media evolution to that of life forms evolving from ocean to land, where addition and diversification, not supplantation, occurs.[6]

Platform as a Service (PaaS):

PaaS enables websites and applications to be launched into the Internet; it facilitates user web creation, multiple users, development collaboration, and subscription management. Examples include Microsoft Azure and Google App Engine.[7]

Infrastructure as a Service (IaaS):

IaaS is the base or hardware infrastructure where the cloud is stored. This includes "servers, processing power, storage, networks, and other physical resources."[8] Examples include Amazon Web Services, such Amazon's "Elastic Cloud Compute" (EC2).[9]

1.2 Cloud Providers' Treatment of User Data, Pre-Revelations:

Cloud platforms have been notoriously passive in responding to US government requests for users' personal data, unquestioningly handing over users' information.[10] In fact, cloud servers' business models are predicated on mass mining of user data for marketing profits. To maintain profitability under this business model, user default settings automatically share user data, often without users' knowledge. Most users do not know or take the time to change their preferences to protect their privacy. Even if individual user settings are changed, there is no way to know if these preferences are being honored. In fact, it has been documented that companies routinely circumvent users' privacy preferences indicated on other businesses' websites, violating Federal Trade Commission (FTC) regulations.[11] This business model of data mining makes SaaS end-user cloud computing a particularly suitable medium for NSA surveillance.

1.3 NSA Surveillance in Cloud Computing, Pre-Revelations:

As a result of the USA Patriot Act, NSA surveillance infiltrated even more deeply into the Americans' personal information through cloud computing. After 9/11, the USA Patriot Act expanded US government surveillance capabilities. The government could now tap into business records,[12] library borrowing histories, Internet habits,[13] and user information through cloud services by American owned companies in any global location.[14] The USA Patriot Act extends US government surveillance capabilities beyond US soil to US-owned cloud computing companies, like Google and Microsoft, that house, for example, European data on European soil.[15] The ramifications of this NSA

surveillance on cloud computing has clear effects on business decisions regarding cloud computing.

1.4 Governments and Cloud Computing, Pre-Revelations:

Governments have been both motivated and cautious to board the exploding trend in cloud computing, as China demonstrates. While China is rushing to catch up to the cloud computing revolution,[16] Chinese skepticism of data security by non-Chinese governments has limited future development plans to clouds owned, operated, and housed solely on Chinese soil.[17] Economic powerhouse China represents only 3 percent of the world's cloud computing and has designated $1.5 billion to a 5-year prioritization plan (2011-2015), to catch up to the rest of the world in cloud computing.[18] However, China will not generally board other countries' clouds, but, rather will develop and utilize its own private clouds.[19] Microsoft, the first Chinese accredited international cloud, just offered its cloud to China in June 2013, with its Windows Azure platform together with Chinese data center service provider, 21 Vianet. Meanwhile, Baidu Cloud boasted 70 million users by mid 2013, a 350% increase from 20 million users less than one year before.[20] The independent behemoth of China's Baidu Cloud will surely be an international force and powerhouse in years to come. Current virtually borderless cloud computing may become more nationalized and fragmented as powerful countries like China take cloud computing into their own hands.

1.5 Businesses and Cloud Computing, Pre-Revelations:

Even before Snowden's revelations, cloud computing stored business and client data with third party providers, in various unreported countries, creating concern for businesses of data surveillance through the USA Patriot Act. Thus, cloud storage is potentially problematic for multinational businesses, since absence of location knowledge violates the EU Data Protection Directive tenets. The EU Directive mandates that data not be transferred from Europe to the United States, where regulations do not meet European standards. Furthermore, the most common method of complying with the requirements of this EU Directive—the US Safe Harbor Program— is rendered useless in cloud computing, where data can be stored anywhere in the world, outside of both Europe and the United States.[21]

Further, the fear of the USA Patriot Act's unfettered surveillance powers has prompted European IT companies to market their services by emphasizing data storage limitation on European-only sites.[22] Yet, it will be shown later that Snowden's revelations have brought these fears and business reactions to new heights.

1.6 Whistleblower/Leaker, Edward Snowden, Pre-Revelations:

An NSA colleague classified enigmatic high-school dropout Snowden[23] as "a genius among geniuses."[24] Snowden's political leanings were indicated by his vote for a third party candidate in the 2008 presidential election. Snowden said he wanted to blow the whistle on the NSA at the time, but waited in hopes that Obama would bring the change he promised the American voting public.[25]

Snowden gave up his comfortable life in Hawaii when he unveiled NSA secrets to the world through the Guardian, faced accusations of treason, and became a fugitive from the United States government. His life in Hawaii included his reported $200,000/year salary as an NSA contractor for a private sector company, Booz Allen.[26] In March 2013, just two months before his NSA revelations, Snowden is said to have taken a pay cut from a previous job to join Booz Allen, in order to have greater access and collect information on the NSA more efficiently,[27] having planned his NSA revelations well in advance.

1.7 Circumstances Surrounding Revelations

In May 2013, Snowden shocked the world, revealing the invasive and pervasive level of United States governmental surveillance, an internationally relevant issue in the virtually borderless world of cloud computing. Both the circumstances surrounding Snowden's revelations and his stated motivations should be understood to evaluate their credibility.

Snowden's NSA revelations were broad reaching and stunning, bringing to light a deeper understanding of covert NSA activities, particularly in cloud computing. Snowden revealed the existence of PRISM and other NSA programs that mass mined American citizens' personal communications, including phone calls, emails, and social networking, to a shocking level.[28] Through PRISM, the NSA can access individuals' "emails, video chats, pictures and more".[29] Cloud computing— including Gmail's email and photo attachments, Gchat, Facebook, and Twitter— is a major platform for these NSA-mined modes of communication.

Snowden justified his actions by citing the US Constitution, the Universal Declaration of Human Rights, and the Nuremburg Principles. He declared: "I didn't want to change society. I wanted to give society a chance to determine if it should change itself".[30] The US constitution's 4th amendment affirms "the right of the people to be secure in their persons, houses, paper, and effects, against unreasonable searches and seizures".[31] Its 5th amendment asserts "…nor shall private property be taken for public use, without just compensation".[32] The Universal Declaration of Human Rights sustains "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[33] Snowden cited these amendments and quotations to demonstrate his opinion of the criminality of the United States' indiscriminate seizure of private data.[34] He continued:

> I believe in the principle declared at Nuremberg in 1945: "Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring."[35]

By citing the US constitution and Universal Declaration of Human Rights, Snowden discusses his opinion of the unconstitutionality of NSA surveillance; by quoting the Nuremberg principle, Snowden justifies his own breach of domestic law for the purpose for the greater good. Snowden, in his video interview to *The Guardian*, said he chose against making anonymous revelations, as he felt it important that the public know his background and motives to judge the quality and reliability of his information.[36]

Despite his justifications, the following month, June 2013, Snowden was charged with espionage by the government of the United States and his passport was invalidated. However, non-US airport officials turned a blind eye, and Snowden is currently living in Russia under a temporary one-year asylum. His media influence continues, as he has since been on Russian television, interviewing Russian President Vladimir Putin.[37] Snowden and his NSA revelations remain a visible presence and will continue to influence decisions regarding cloud computing.

2. Impact of Snowden's NSA Revelations on Cloud Computing

The impact on cloud computing of Snowden's NSA revelations was transformative and marked the threshold of a new era, bringing both benefits and difficulties. Although privacy concerns existed before Snowden's revelations, the new flurry of debates has proliferated in light of the controversy.[38] Benefits of the Snowden revelations include heightened awareness, lively discussion of individual privacy rights, trending to greater transparency in data requests, and open debate to create international systems protecting public data privacy. Difficulties of the revelations include international mistrust in American cloud computing causing massive pullout and economic strife on American tech companies and, therefore, the American economy at large.

2.1 Government Reaction: Domesticating Cloud Servers

International governments, such as Brazil, are now wary of storing their data in United States based clouds. In a direct reaction to the Snowden revelations' emphasis on

widespread digital surveillance,[39] Brazilian President Dilma Rousseff made clear that Brazil will reduce dependence on US based cloud platforms to avoid NSA surveillance.[40] This trend to transfer data to domestic servers will shape the architecture of cloud computing for years to come, fragmenting surveillance from US to regional sources.[41]

Germany is another important country steering clear of cloud services in the United States. Germany Chancellor Angela Merkel recommended that Germans use in-country instead of American online services, as a result of the Snowden revelation that the NSA had monitored her phone conversations. Germany even recommended, through Interior Minster Hans-Peter Friedrich, that Germans stop using Facebook and Google to avoid NSA espionage.

American cloud services are already suffering because of governments' fears of US based cloud computing. In fact, in light of the NSA revelations, IBM is spending over $1 billion to construct data centers overseas, Microsoft has already lost substantial business, including the country of Brazil, and non-US tech companies are gaining business lost to American businesses as a result of the fear of storing data in the United States under NSA surveillance.[42] Nations' regulations and recommendations will directly affect corporate capabilities and business decisions.

2.2 Business Reaction: The "Snowden Effect"

Snowden's NSA revelations have produced the "Snowden Effect:" a heightened awareness of American espionage that is magnifying businesses wary of cloud computing

that may ultimately store data in the United States.[43] "The impact of the Snowden leaks could threaten the future architecture of the modern Internet," writes Gerry Smith of the World Post.[44] He continues, "In recent years, computing power has shifted from individual PCs to the so-called cloud—massive servers that allow people to access their files from anywhere."[45] With Snowden revealing NSA espionage on US-based cloud companies like Google and Yahoo, the Snowden effect has created a loss of trust in businesses with US cloud providers.[46]

In just a few months of Snowden's revelations, a full 10% of non-American companies have withdrawn their business from American cloud businesses, according to a survey by Cloud Security Alliance.[47] A study by the Information Technology and Innovation Foundation projects that American cloud services over the next three years could see as loss of $35 billion.[48] To compete in the global economy, it is vital the American privacy rules be changed to match European privacy rules.

Corporate leaders are pulling out of the cloud, and cloud providers must act quickly to regain trust and reestablish business. In NSA Aftershocks, a study by NTT Communications, 90% of it 1,000 "decision makers" surveyed in the UK, Hong Kong, France, Germany, and, notably, the United States have been affected by the Snowden revelations in decisions related to cloud usage. A substantial 62% noted they did not submit their companies' Information and Communications Technology (ICT) into the cloud, because of the Snowden revelations.[49] In the Snowden Effect aftermath, only those

cloud providers that act quickly and provide consumers with all-important "data integrity, governance and security" will survive the brave new world of cloud computing.

2.3 Organization Reaction: A Proactive Approach

Organizations are now taking a proactive approach to protecting their own and the public's privacy from the US government, in light of the Snowden revelations. For example, the Electronic Privacy Information Center (EPIC) took the fight to reverse the NSA's demand for all of Verizon's customers' telephone records all the way to the US Supreme Court.[50] Other non-profit advocacy groups sent letters to NSA Director and US Trade Representative, asking if their organizations were under surveillance by the NSA.[51]

One shocking effect of the Snowden revelations on organizations is a suggestion to return to pre-technological means of communication: the carrier pigeon and "sneakernets." Anthony Judge, former Assistant Secretary-General of the Union of International Associations,[52] a "non-profit, apolitical, independent, and non-governmental" organization,[53] suggested the use of carrier pigeons. Judge cited a example of a British carrier pigeon that delivered a five-minute video, flying 75 miles, faster than is taken to upload from a small farm onto YouTube.[54] In the same vein, "sneakernets" are also a possible way around ubiquitous online surveillance. Sneakernets are people who hand-deliver sensitive data via USB drives to circumvent online intelligence, as was exemplified by courriers to Osama Bin Laden, North Korea and Cuba.[55] These extreme concerns for privacy filter down through every layer of society.

2.4 Individual Reaction: New Concern for Privacy

The Snowden effect is showing itself in extreme concern for privacy among individuals. The Snowden revelations may be bringing back the idea of individual privacy as a social norm.[56] A Harris Poll in November 2013 revealed that 80% of individuals changed their social media privacy settings, most in the previous six months.[57]

As a result of the Snowden revelations, individuals' interest has also increased dramatically on privacy tools, including anonymizers and encryption. However, only the most technically savvy makes use of these techniques. This leaves the vast majority of the general public unprotected.[58] Individuals' search for encryption techniques has exploded, as indicated by the quadrupled 139 million hits on the encryption download page of Tor (The Onion Router) encryption service in 2013. While Snowden also revealed in 2013 that the United States government is working on decrypting Tor, slides revealed by Snowden also show the US government's frustration in breaking Tor's code: "We will never be able to de-anonymize all Tor users all the time. With manual analysis we can de-anonymize a very small fraction of Tor users."[59] True to Tor's name, short for "the onion router," Tor's layers increase the layers of protection substantially. After analyzing the revealed NSA slides with *The Guardian*, cybersecurity expert Bruce Schneier concluded, "Encryption works… The NSA can't break Tor."[60] Nonetheless, until encryption is made user friendly, only a minority will use it, and citizens' privacy will remain unprotected.

2.5 Cloud Providers' Changing Treatment of User Data:

Protection of User Data and Transparency of Surveillance

In the aftermath of Snowden's revelations, cloud providers are now showing signs of standing up to government requests for user data and providing greater transparency of government requests. For example, Twitter is now being praised for its challenging government requests for user identities, in particular the identity of an Occupy Wall Street protester.[61] In addition, Twitter notifies users of governmental requests for their information in a more transparent fashion than other public platforms.[62] In another move for greater transparency, in June 14, 2013, Yahoo filed to have court papers from NSA's 2008 PRISM gathering of Yahoo users' data, unsealed and open to the public. Prior to Yahoo's request, the last unsealing of governmental requested records was ordered over a decade earlier, in a Patriot Act case in 2002.[63]

Encryption of telephone, texts, email, and video chat is now being proactively marketed to consumers wary of government interception, especially on cloud computing mediums. Yet, despite these baby steps, most cloud companies lack both resources and initiative to protect our individual rights, leaving us to navigate the murky waters against these titanic forces on our own.[64] A more organized effort is necessary to create a safety net policy to protect individual privacies.

3. Implications and Suggestions

3.1 International Consortium Agreement:

Leveling the Playing Field of Cloud Computing

As espionage is pervasive in many countries, an international consortium agreement must be implemented to institute policy reform internationally and level the playing field in cloud computing. While the spotlight is now shed on United States counter-terrorism intelligence, other countries participate in the same intelligence gathering of individuals' data. In fact, *The Guardian* reported that Britain's version of the NSA, known as the GCHQ, has been duplicating the NSA efforts through a system set up by the NSA.[65] Similar to the United States' PRISM program, the United Kingdom runs its own Tempora program that work in conjunction with the United States' Prism program to tap cable and networks on anything traveling through the Internet, via an ability called Upstream. This is then stored and immediately accessible through a database, XKeyscore.[66] This means that efforts to keep data outside the US could be fruitless, as data would simply be mined by other resident cloud countries.

To restore trust in cloud computing, loopholes in anti-espionage legislation must be identified and solutions found. For example, as revealed in Snowden's documents, Five Eyes—an agreement among the five Anglophonic countries of Australia, Canada, New Zealand, the United Kingdom, and the United States—enables the countries to skirt domestic anti-espionage laws by spying on each other's citizens and reporting their

findings.[67] A level playing field and fair play must be instituted for equitable international relations and global growth.

3.2 Balanced Policy: National and Individual Security

Anti-terrorism laws must be structurally balanced with preservation of privacy rights. Although it is discomforting to have our individual rights to freedom violated, the massive data mining system, PRISM has prevented a planned suicide bombing from taking place in New York subways in 2009.[68] On the other hand, Senators Wyden (D-Ore) and Mark Udall (D-Colo) fail to see any tangible anti-terrorism benefit from the data mining of the Patriot Act.[69] With such controversy surrounding the efficacy and risks of data mining, transparency is needed to protect individuals' privacy. The current lack of transparency was demonstrated when the government refused to reveal the intercepted communication of Americans, even after repeated requests by Congress.[70] Balanced legislation, considering both national and individual security, and transparency is essential for the national, individual, and, thus, cloud computing needs.

3.3 Transparency: Repair Public Trust

Transparency of government surveillance is essential to repair public trust. To this end, obscured data, inconsistent data, and weak internationalization must also be mended. Data can be "obscured" by issuing lists that combine national security and domestic criminal requests, as recently demonstrated by Facebook and Yahoo! Combined, proper analysis of each independent list is "obscured."[71] Therefore, security and domestic criminal requests must be issued separately for clear analysis. Data can be "inconsistent"

by varying definitions on terms like "user" or "court order" by various companies.[72] Thus, a consistent system of definition of terms must be instituted across the board for accurate comparison and analysis. "Weak internalization" refers to the fact the companies supply requests for information from only the United States and not other countries.[73] Thus, companies must supply requests from any country requesting information. By separating national security lists, issuing a consistent definition of terms across companies, and supplying requests to the public from any country requesting information, transparency will be greatly improved.

3.4 Legislation: Update with Technology

Antiquated legislation struggles to stay relevant to technological advances and must be modernized to meet user privacy needs. For example, the Stored Communications Act (SCA) was established before the advent of both high-speed Internet and massive free cloud storage and can be easily abused by United States law enforcement. Using this outmoded SCA legislation, law enforcement can issue a subpoena without court order and obtain "a person's name, physical address, IP addresses, data about when she signs on and off of an online service, and her payment processing information."[74] This wealth of information is available without court supervision or notification of the target of investigation. If law enforcement notifies its target, it can then access virtually all the target's emails.[75] Policies and laws must be updated and made relevant to current cloud computing technologies, in order to continue to preserve individual privacy rights.

3.5 Data Encryption: User Friendly

Data encryption must be made user friendly and cloud compatible to enable widespread use and public trust in cloud computing. While secure data encryption is widely available—including PGP for email encryption, OTR for instant messaging, and Redphone for Internet telephony—the procedure to set up and use these systems has been convoluted, so the general public, valuing convenience, continues to opt out of these systems. In addition, encryption carries other issues, such as unrecoverable user passwords, interference with useful features by cloud platforms like Gmail to search emails and Facebook to index and render searchable posts, and the requirement that both sender and receiver install the technically challenging encryption systems. Therefore, even when users have encryption installed, they generally use unencrypted methods, since their contacts are not encryption equipped.[76] Encryption must be made user-friendly and cloud compatible, so that the public will use it, restoring trust in cloud computing.

3.6 Academia: Research Solutions to Implement Effective Policy

Academia can research issues, provide a platform to find solutions, and communicate through the appropriate channels to effect public policy and private solutions. As the Berkman Center for Internet & Society at Harvard University is demonstrating by its first annual edition of The Internet Monitor,[77] a symposium of diverse panelists can collaborate to work towards raising public awareness and finding solutions. These solutions can reinvigorate cloud computing in the post-Snowden era.

4. Conclusion

Cloud computing in the post-Snowden era is now at a crossroads where the reinstitution of public trust on a global scale is instrumental for continued growth, particularly in the United States, but also globally. A conscious balance between both national and individual needs must be legislated, internationally and domestically. The pre-Snowden era has been characterized by unbridled growth with only a wary side-glance at the dangers of privacy issues. The Snowden revelations have offered us an opportunity to reexamine the fundamental needs for individual security and privacy, while balancing the need for national security. The post-Snowden trend toward international fragmentation and non-participation in cloud computing can be redirected by implementing legislation, transparency, and privacy protections all designed to restore public trust.

The future of healthy international cloud computing requires research and implementation of solutions. Suggestions include an International Consortium Agreement that would level the playing field, policy that balances national and individual security, transparency to repair public trust, legislation that is updated with technology, data encryption that is user friendly and cloud compatible, and academia research for continued research and policy recommendations for implementation. A single nation, as well as the international community, is a living organism. The state is the body and the individuals are its cells, forming an interdependent ecosystem. The body can no more thrive without the health of its cells than cells can thrive without the health of the body. In this way, the state can no more flourish without the well-being of its individuals than

individuals can flourish without the well-being of the state. For this ecosystem to flourish, a balancing act is needed between national security and individual security. Only by instituting this balance between the state and its individuals can healthy global growth continue in cloud computing.

REFERENCES

[1] Faris, Robert, and Rebekah Heacock. "Introduction." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 5. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[2] Id. at 5.

[3] "Cloud." *Oxford English Dictionary* Online. HUL Access/2.0. Accessed January 7, 2015. http://www.oed.com.ezp-prod1.hul.harvard.edu/view/Entry/34689?redirectedFrom=cloud+computing#eid189443962.

[4] Gasser, Urs. "Cloud Innovation and the Law: Issues, Approaches, and Interplay." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013). Berkman Center. March 17, 2014. http://cyber.law.harvard.edu/node/9070.

[5] Kelly, John. "Three Generations of the Networked Public Sphere." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 14. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[6] Id. at 14.

[7] Kepes, Ben. "Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS." *Rackspace Support*. October 22, 2013: 7. http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas.

[8] Gasser, Urs., "Cloud."

[9] Id.

[10] Topelson, Dalia. "The New Guard." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 56-7, 56. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[11] Soltani, Ashkan. "The Privacy Puzzle: Little or No Choice." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 81. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_Reflectionsont heDigitalWorld.pdf.

[12] Finn, Peter, and Ellen Nakashima. "Obama Defends Sweeping Surveillance Efforts." *The Washington Post*. June 7, 2013. http://www.washingtonpost.com/politics/obama-defends-sweeping-surveillance-efforts/2013/06/07/2002290a-cf88-11e2-9f1a-1a7cdee20287_story.html.

[13] Risen, James, and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." *The New York Times*. December 16, 2005. http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

[14] Finn, Aidan. "A Factual Analysis of Cloud Computing VS The USA Patriot Act." *Aidan Finn, IT Pro*. Accessed April 25, 2014. http://www.aidanfinn.com/?p=11187.

[15] Id.

[16] Wu, Mark. "China Moves to the Cloud." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 34-7. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[17] Id. at 36.
[18] Id. at 34.
[19] Id. at 34.
[20] Id. at 35.

[21] Mathews, Kristen J. "Privacy Issues When "Computing in the Cloud"." *Privacy Law Blog*. November 26, 2008. http://privacylaw.proskauer.com/2008/11/articles/european-union/privacy-issues-when-computing-in-the-cloud/.

[22] Overby, Stephanie. "The Patriot Act and Your Data: Should You Ask Cloud Providers About Protection?" *CIO*. January 20, 2012.

http://www.cio.com/article/2400264/government/the-patriot-act-and-your-data--should-you-ask-cloud-providers-about-protection-.html.

[23] Connor, Tracy. "What We Know About NSA Leaker Edward Snowden." *NBC News*. June 10, 2013. http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden?lite.

[24] Greenberg, Andy. "An NSA Coworker Remembers The Real Edward Snowden: 'A Genius Among Geniuses'." *Forbes*. December 16, 2013. http://www.forbes.com/sites/andygreenberg/2013/12/16/an-nsa-coworker-remembers-the-real-edward-snowden-a-genius-among-geniuses/.

[25] MacAskill, Ewen. "Edward Snowden, NSA files source: 'If they want to get you, in time they will.'" *The Guardian*. June 10, 2013. http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why.

[26] Connor.

[27] Shane, Scott, and David E. Sanger. "Job Title Key to Inner Access Held by Snowden." *The New York Times.* June 30, 2013. http://www.nytimes.com/2013/07/01/us/job-title-key-to-inner-access-held-by-snowden.html?pagewanted=all.

[28] Lanchester, John. "The Snowden Files: Why the British Public Should Be Worried About GCHQ." *The Guardian*. October 3, 2013.

http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester.

[29] Abdollah, Tami. "Court Sides with Yahoo in Data Collection Case." *AP Party*. Bigstory.ap.org. July 16, 2013. http://news.yahoo.com/court-sides-yahoo-data-collection-case-005743639.html.

[30] Gellman, Barton. "Edward Snowden, After Months of NSA Revelations, Says His Mission's Accomplished." *The Washington Post*. December 23, 2013. http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

[31] "Fourth Amendment." *Legal Information Institute*. Cornell University Law School. Accessed April 25, 2014. http://www.law.cornell.edu/wex/fourth_amendment.

[32] "Fifth Amendment." *Legal Information Institute*. Cornell University Law School. Accessed April 25, 2014. http://www.law.cornell.edu/wex/fifth_amendment.

[33] "Article 12- Universal Declaration of Human Rights." *Archives of the International Council on Human Rights Policy*. ICHRP. http://www.ichrp.org/en/article_12_udhr.

[34] Our Foreign Staff. "Edward Snowden's Statement to Human Rights Groups in Full." *The Telegraph*. July 12, 2013.

http://www.telegraph.co.uk/news/worldnews/europe/russia/10176529/Edward-Snowdens-statement-to-human-rights-groups-in-full.html.

[35] Id.

[36] Greenwald, Glenn. "NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society That Does These Sort of Things' – Video." *The Guardian*. June 9, 2013. http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

[37] Logiurato, Brett. "Snowden Makes Stunning Appearance On Putin TV Interview in Apparent PR Stunt." *Business Insider*. April 17, 2014. http://www.businessinsider.com/edward-snowden-putin-q-a-surveillance-2014-4.

[38] Schulz, Wolfgang, "After Snowden: Toward a Global Data Privacy Standard?" *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 30. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[39] Faris at 5.

[40] Id. 6.

[41] Faris, 6.

[42] Miller, Claire Cain, "Revelations of NSA Spying Cost US Tech Companies." *The New York Times.* March 21, 2014.

http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

[43] Smith, Gerry. "“Snowden Effect” Threatens US Tech Industry's Global Ambitions." *The World Post.* Yale Global Online Magazine. January 28, 2014. http://yaleglobal.yale.edu/content/%E2%80%9Csnowden-effect%E2%80%9D-threatens-us-tech-industrys-global-ambitions.

[44] Id.
[45] Id.
[46] Id.
[47] Id.
[48] Id.

[49] Dunn, John E. "'Snowden Effect' Has Changed Cloud Data Security Assumption, Survey Claims." *Techworld*. April 16, 2014. http://www.techworld.com/news/security/snowden-effect-has-changed-cloud-data-security-assumption-survey-claims-3512185/.

[50] Acohido, Byron. "Snowden Effect: Young People Now Care About Privacy." *USA Today*. November 18, 2013. http://www.usatoday.com/story/cybertruth/2013/11/13/snowden-effect-young-people-now-care-about-privacy/3517919/.

[51] Id.

[52] Troumbley, Rex. "Flying Past Filters and Firewalls: Pigeons as Circumvention Tools?" *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 83-4.

http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[53] "Union of International Associations." UIA. Accessed April 20, 2014. http://www.uia.org/.

[54] Troumbley at 83.

[55] Id. 83.

[56] Acohido.

[57] Id.

[58] Etling, Brett. "Citizens as Actors." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 68. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[59] Lawrence, Dune. "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built." *Bloomberg Businessweek*. January 23, 2014. http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency.

[60] Id.

[61] Weiner, Rachel. "Twitter Earns Plaudits for Privacy Amid NSA Controversy." *The Washington Post*. June 7, 2013. http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/07/twitter-earns-plaudits-for-privacy-amid-nsa-controversy/.

[62] Id.

[63] Abdollah.

[64] Topelson at 56.

[65] Finn, P.

[66] Lanchester.

[67] Id.

[68] Finn, P.
[69] Id.
[70] Id.

[71] Budish, Ryan. "Transparency Reporting." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): 54. http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.

[72] Id. at 54.
[73] Id at 55.
[74] Id at 54.
[75] Id.

[76] Lee, Timothy B. "NSA-proof Encryption Exists. Why Doesn't Anyone Use It?" *The Washington Post*. June 14, 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/.

[77] Gasser, Urs. "About this Report." *Internet Monitor 2013: Reflections on the Digital World* 1 (2013): Preface.

http://blogs.law.harvard.edu/internetmonitor/files/2013/12/IM2013_ReflectionsontheDigitalWorld.pdf.