Government Surveillance and Its

Impact on the Global Business Community

Samuel Roth

Principles of Entrepreneurship

Dr. Tammy Schakett

14 March, 2014

In June 2013 news organizations *The Guardian* and *The Washington Post* began to publish classified documents from the National Security Association (NSA) about massive operations to collect the personal information of both Americans and foreigners, with the only clear motive being that of countering domestic terrorism. [Greenwald, 2013] Since then, the United States government has tried to justify its actions while simultaneously tracking down and bringing Edward Snowden to justice. Throughout the entire debacle, the government has received harsh criticism from not only its own citizens, but the companies based in the country as well. American companies were placed in an awkward position in the global business community. They lost the trust of their customers, as well as the trust of other companies that they did business with.

# **Domestic Consequences**

The initial unraveling of the Snowden case was only the beginning of a strenuous battle between the United States government and various different bodies of people. United States citizens called for the elimination of the National Security Agency and the resignation of individuals who knew about the agency's activity [France-Presse, 2014]. The news spread like wildfire through both domestic and international media, and suddenly, the concept of information privacy was one that everyone was talking about. People likened the situation to the beginning of an Orwellian surveillance state [Rushe, 2013].

Edward Snowden's revelations continued long after the initial release via *The Guardian* and the *Washington Post*. Just one day later, on June 6, 2013, it was revealed that the National Security Agency was collecting data by tapping into the databases of popular tech companies such as Google, Facebook, Microsoft, and Apple [Greenwald, 2013]. Many of these companies

banded together in an effort to regain the trust of their customers. They argued loudly and publicly for additional government transparency and for overhaul of the National Security Agency's surveillance operations. Some tech firms even claimed that they were unaware of the agency's activities, and that they accessed their databases illegally.

## **International Consequences**

Other significant revelations confirmed that the National Security Agency was not limiting its data collection to the United States. The nation's relationships with various other countries, including allied countries, were put under enormous tension after it was brought to light that the agency collected data on foreign leaders [Greenwald & MacAskill, 2013] and foreign nationals [NBC News, 2013]. This was detrimental in the government's effort to return Snowden to the United States, as Snowden was ultimately offered annual asylum in Russia [Heritage & Holland, 2013].

The companies involved in the debacle faced significant criticism from their global business partners as well. While they are based in the United States, all of the giant tech firms that were impacted have significant global operations. Foreign interests that were doing business with the U.S. tech industry were suddenly pulling out of negotiations, notably China [Miller, 2013]. The companies also lost many of their foreign customers.

### **Good Intentions?**

As the Snowden leaks spread like wildfire, it became clear that the United States could not deny the allegations, and instead had to respond to them both promptly and strongly. The problem that the agency faced was finding a balance between achieving domestic security and

plain abuse of power. Ultimately, President Barack Obama said that he would consider recommendations to reform the National Security Agency [Shapiro, 2013].

The process to reform the agency is one that continues to this day. It is important to understand *why* the government would operate in this manner, which is ultimately to protect the American public against terrorism, both domestic and abroad. While the American public may feel that the government should not necessarily have direct access to their Tweets, their Facebook posts, or otherwise - which is a valid truth - it is necessary to consider the lengths that the intelligence community goes to to keep the nation safe. This is an issue that all countries must consider. It is interesting to note that the public was outraged to learn that professionals (who have been through intense background checks) have access to this information, while they have no trouble posting the most intimate moments of their life to social networks in the first place. Very ironic, considering the fact that the founder of Facebook, Mark Zuckerberg, admitted to calling individuals who trust him with their personal information "dumb fucks" [Tate, 2010].

### **The Silver Lining**

Ultimately, the entirety of America was a victim of its own negligence. However, in some peculiar way that we aren't entirely aware of, we do benefit from the actions taken to protect against acts of terrorism. It cannot be denied that the employees of the National Security Agency have had more background-screening than those of, for example, Facebook.

American corporations have lost business due to the revelations, and have had to fervently advocate reform in order to regain the trust of their customers. The events have also caused these companies to be more open about how they themselves handle the information their customers provide to them.

# **Moving Forward**

One lesson everyone can take away from this case is that they should be careful about what information they share online. While the social revolution is surely under way, a frightening majority of the consumers of these networks do not understand that the information they share on the Internet cannot be removed, regardless of what controls social networks say they have. One cannot prevent people from seeing and saving something he or she posts, to use it against them at a later date. This is an issue that will have a significant impact on future generations, and is not limited to just Americans. As the world becomes more intricately connected, we must all be properly educated on the basics of safe and secure Internet usage.

Businesses, both domestic and abroad, have learned from this incident as well. As the world begins to become more aware of the subject of information privacy, companies must take steps to protect the information they are trusted with - not only from hackers, but from governments as well. In reality, the idea of information privacy is an entirely new category of ethical business behavior. Businesses that do not actively pursue the trust of their customers will ultimately lose them.

#### References

- Ball, J. (2013, October 25). NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*. Retrieved February 9, 2014, from <a href="http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls">http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls</a>
- France-Presse, A. (2014, January 23). U.S. privacy board: NSA mass surveillance illegal and should be shut down. *The Raw Story*. Retrieved February 9, 2014, from http://www.rawstory.com/rs/2014/01/23/u-s-privacy-board-nsa-mass-surveillance-illegal-and-should-be-shut-down/
- Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved February 8, 2014, from <a href="http://www.theguardian.com/">http://www.theguardian.com/</a> world/2013/jun/06/nsa-phone-records-verizon-court-order
- Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved February 8, 2014, from <a href="http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data">http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data</a>
- Heritage, T., & Holland, S. (2013, August 1). Russia gives Snowden asylum, Obama-Putin summit in doubt. *Reuters*. Retrieved February 9, 2014, from http://www.reuters.com/article/2013/08/01/us-usa-security-snowden-russia-idUSBRE9700N120130801
- Miller, M. (2013, November 14). The NSA Leaks Have Been Crushing US Tech Sales In China. Business Insider. Retrieved February 9, 2014, from http://www.businessinsider.com/nsa-leaks-hurting-us-tech-sales-in-china-2013-11
- Rodden, J. (2002). *George Orwell: the politics of literary reputation*. New Brunswick, N.J.: Transaction Publishers.

- Rushe, D. (2013, September 23). NSA surveillance goes beyond Orwell's imagination. Alan Rusbridger. *theguardian.com*. Retrieved February 8, 2014, from <a href="http://www.theguardian.com/world/2013/sep/23/orwell-nsa-surveillance-alan-rusbridger">http://www.theguardian.com/world/2013/sep/23/orwell-nsa-surveillance-alan-rusbridger</a>
- Shapiro, A. (2013, November, 13). How Obama's Response To NSA Spying Has Evolved. *NPR*.

  Retrieved February 9, 2014, from <a href="http://www.npr.org/blogs/itsallpolitics/">http://www.npr.org/blogs/itsallpolitics/</a>
  2013/11/13/245037300/how-obamas-response-to-nsa-spying-has-evolved
- Tate, R. (2010, September 13). Facebook CEO Admits To Calling Users 'Dumb Fucks'. (n.d.). *Gawker*. Retrieved February 9, 2014, from http://gawker.com/5636765/facebook-ceo-admits-to-calling-users-dumb-fucks
- US coping with furious allies as NSA spying revelations grow. (2014, February 3). *NBC News*.

  Retrieved February 8, 2014, from <a href="http://www.nbcnews.com/news/us-news/us-coping-furious-allies-nsa-spying-revelations-grow-v21209499">http://www.nbcnews.com/news/us-news/us-coping-furious-allies-nsa-spying-revelations-grow-v21209499</a>