CASE 1 NSA: National Surveillance Agency?

In the 1950s, shortly after the end of World War II, President Harry S. Truman oversaw the organization of a secret security and intelligence organization, tasked with gathering and analyzing intelligence data in defense of the interests and operations of the United States and its government. The organization—named the National Security Agency (NSA)—has since grown to become one of the largest intelligence organizations in the world, with an estimated workforce of around 40,000 employees and annual budget of nearly US$11 billion (these types of information about the NSA are classified). The NSA has been involved in gathering intelligence on a wide range of issues and individuals, from the Vietnam War to Martin Luther King, Jr. to the post-9/11 War on Terror. By design, many of the NSA's successes are classified and not known to the general public, but the agency has been credited with providing key intelligence in support of major military and investigatory operations over the past several decades.

In its relentless pursuit of intelligence to defend U.S. national interests, the NSA has embraced technology and the vast amounts of digital information available across the globe. In late 2013, a series of disclosures of classified internal NSA documents revealed the extent of the NSA's spying activities. Most of these disclosures were provided by a former NSA contractor named Edward Snowden. These documents revealed that the NSA regularly intercepts the telephone and Internet communications of over a billion people worldwide. The NSA tracks the locations of hundreds of millions of cell phones per day. The organization reportedly has access to at least some communications made via services provided by AOL, Google, Microsoft, Facebook, and Yahoo, and collects hundreds of millions of contacts lists from personal e-mail and instant messaging accounts every year. The NSA also collects and stores cell phone call records from major cell phone providers. These surveillance activities have not been limited to countries considered to be enemies of the United States—they include longtime friendly countries such as France, Germany, and Spain. Perhaps most unsettling for U.S. citizens is the fact that NSA surveillance has also been targeted at U.S. citizens within U.S. borders, which appears to many as a clear violation of the Foreign Intelligence Surveillance Act of 1978—a law designed to limit the practice of mass surveillance in the United States.

Given that much of the NSA's activities are classified, it is hard to know how effective these massive surveillance practices have been in defending U.S. national interests and U.S. citizens. To some extent, many citizens likely expect the government to engage in spying and other intelligence-gathering practices to protect the public against terrorism, crime, or other dangers. To this end, the NSA reportedly provides foreign intelligence to the Central Intelligence Agency (CIA) regarding terrorist activities, and domestic intelligence to the Drug Enforcement Administration (DEA) and Federal Bureau of Investigation (FBI) regarding drug and other criminal activities. But just how much intelligence-gathering the NSA should engage in, and from whom, is a matter that has come under strong debate. Judging by the public outcry in response to the revelations from Edward Snowden's leaked documents, many people, both within and outside of the United States, believe that the NSA has gone too far.

In some sense, the NSA surveillance activities are little more than advanced business intelligence initiatives. In the modern world, we leave digital footprints in nearly all of our daily activities, from e-mail to text messages to phone calls to social media. The NSA has developed methods to collect and store this data, much to the consternation of many people now learning of these practices. But many large businesses engage in similar activities, perhaps not on the same scale, but with equal disregard for the privacy of the people being tracked. Google, Facebook, and many online advertising networks that you have likely never heard of go to great lengths to record where we go and what we are watching, listening to, and reading. These activities provide powerful business opportunities for segmented marketing, and they are the revenue source supporting many of the online services that we enjoy for free.

So how do we balance the privacy issues caused by surveillance—both by governments and online companies—with the valid purposes that these organizations use to justify their activities? Would you rather that the U.S. government miss the opportunity to stop a terrorist organization before it strikes because the NSA stopped monitoring electronic communications? Would you be willing to pay a yearly subscription fee to Google in order to use its search engine or e-mail services? Would you be willing to pay a fee each time you "friended" someone or posted a new photo album on Facebook? These are extreme examples, but they highlight the conflict inherent to any discussion that tries to weigh privacy against business intelligence practices. For governments and companies to succeed and provide the services we expect, we may need to become more comfortable with giving up some of our privacy.

Questions

6-48. Do you think that the NSA has gone too far in its surveillance activities? Why or why not?

6-49. What are the pros and cons inherent to data collection for business or national intelligence?

6-50. Propose a set of guidelines for the NSA to direct its surveillance activities in the future.

Based on:

National Security Agency. (2014, May 27). In *Wikipedia, The Free Encyclopedia*. Retrieved May 30, 2014, from http://en.wikipedia.org/w/index.php?title=National_Security_Agency&oldid=610317412.

Shane, S. (2013, November 2). No morsel too minuscule for all-consuming N.S.A. *The New York Times*. Retrieved May 29, 2014, from http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html.