Dr. Burns

English 1010

23 November 2013

Watching In: Self-Surveillance in the Contemporary United States

Privacy — at first glance, most people see this word as describing one's right to be free from observation and disturbance by others; however, upon further examination it means much more. According to author Dylan Love of the *Business Insider*, this word in itself is one of hundreds that flag you as a potential terrorist when typed it in an email. Perhaps this comes as no surprise; since the Obama administration has come into office, citizens of the United States have seen an increasing presence of the National Security Agency (NSA) in the media and their daily lives. The NSA is a subsection of the US government chartered to help protect US national security by producing intelligence information and providing it to the US government. But the methods by which the NSA obtains this intelligence and the levels to which the NSA looks into our personal lives are controversial. In 2009 the National Security Council (NSC) published a cyberspace policy review, which focused on how the government was to protect and promote US security through cyberspace. An important part of the document lays out four key ideas that the US government feels any cyberspace policy should have: governance, architecture, norms of behavior, and capacity building. I will be closely examining each of these key ideas to show how current NSA policies and actions do not coincide NSC policy.

The first idea presented in the policy review is governance. According to the NSC, governance is the idea that a cyberspace policy must make sure that various departments of the government will work with one another when in a cyberspace mission (B-5). To determine if this principle is currently implemented by the NSA, one can look to the NSA's metadata collection process. Authors Ewen Macaskill and Gabriel Dance, of *The Guardian*, explain

metadata as information provided by large wireless communication companies, such as Verizon, concerning client's phone call histories. According to the Obama administration's white paper released on August 9, 2013, metadata is the collection of information on phone calls, such as telephone numbers, where the calls were made, the duration of the calls, and who received the call, not on what was said in the conversation (2). What is most concerning is how this collection of data was kept secret. According to author Glenn Greenwald, also of the *The Guardian*, it was not until the summer of 2013 that the public learned President Obama had allowed this type data collection, started under the Bush administration, to continue. This means that for over 4 years this program was shrouded in secrecy. To quantify this secrecy, authors Macaskill and Dance look to when the Director of National Intelligence, James Clapper, misled congress. The authors talk about how Clapper, when asked if the NSA was collecting data on millions of Americans, responded bluntly with "No, sir." This means either Clapper knew the NSA was collecting all of this metadata and lied directly to congress, or that Clapper truthfully did not know, and had been lied to by a different government official. In either scenario information was kept secret from certain governmental agencies and officials. If information is kept secret, and is specifically left to one group of people, there is no reasonable way we can expect that different departments are working together when it comes to cyberspace missions. Through the evidence provided one can see how the NSA is not incorporating the idea of governance into its policies and actions.

The second idea on which the policy review focuses is architecture. The NSC describes architecture as "understanding and analyzing the following: information you already have, methods of collecting more information, and needs of future programs" (B-5). To understand if the NSA is effectively promoting the idea of architecture in their current policy we will look to

see if the NSA polices and programs have been successful. Authors Peter Bergen and David Sternman, both respected scholars of national security, answer this question in their CNN opinion piece by looking at the number of domestic terrorist attacks prevented by the NSA. The authors state that there have been 42 domestic terrorist plots planned since 2001. Bergen and Sternman then go on to say that 9 of these 42 plots had failed due to an error made by the aggressor, unrelated to the US government knowledge of the plot. That leaves 33 potential attacks left, 29 of which the authors say were stopped by traditional forms of law enforcement, not by NSA surveillance programs. The authors go on to talk about a domestic terrorist plot that was stopped by the surveillance done by the United Kingdoms, not even our own surveillance agencies. The NSA states that its goals are to protect US national security, and to stop potential terrorist attacks; however, the NSA has stopped less than one-eighth of all the domestic terrorist plots over the past twelve year. I believe anybody would have difficulty calling this success. If the NSA is only stopping a minuscule amount of terrorist activity it is clear that the NSA is not effectively understanding and analyzing the information they have, nor the methods by which they collect this information. In addition, how can one reasonably expect that the NSA is addressing the needs for future programs when they cannot handle threats occurring in the present. Because of the lack of success seen in the NSA currently, it is clear there is an absence of architecture in the NSA's policies and actions.

The third key point that the cyberspace policy review talks about is norms of behavior. The NSC describes this as focusing on two needs: addressing laws, regulations, and treaties already in place, and performing actions that help to define good standards of conduct when working on a cyberspace mission (B-5). It would be difficult to make an objective comment on whether the NSA is abiding by current laws and regulations due to the fact that analysis of the

legality of NSA policies is still being debated in congress and is constantly evolving. However, we can look at whether the NSA is defining good standards of conduct and from there make a decision of whether current NSA policy encompasses the idea of norms of behavior. One important standard of conduct that the NSA should be creating is the right and protection to privacy. Since the right to privacy is a civil liberty, it is viewed as extremely important by most citizens of the US. According to authors Macaskill and Dance, 58 percent of Americans believe that the NSA is doing a poor job at protecting their right to privacy; this represents a twelve percent increase since 2011. Not only do Macaskill and Dance show that the public does not believe the NSA is protecting their rights, but they also show that 60 percent of all Americans believe they will be loosing more freedoms in the next decade than they will be gaining. It is clear that if over half of America believes the NSA will be stripping rights away from them in the future, then the NSA is not upholding and creating good standards of conduct. If other governmental agencies see that the NSA is now beginning to strip away freedoms and liberties, who is to say they will not follow close behind? Since the NSA is not upholding a key component defined by norms of behavior it is obvious that the NSA is not effectively incorporating norms of behavior into their current policies and actions.

The fourth and final idea presented in the cyberspace policy review is capacity building. The NSC explains capacity building as the need to make clear all of the recourses, activities, and capabilities a nation must have to become more advance in cyberspace missions (B-5). More specifically the NSC defines these recourses, activities, and capabilities as good research and development, public awareness, and international cooperation (B-5). With the reasons and evidence presented in the paragraph focusing on architecture one can make the assumption that the NSA lacks effective research and development because of their failure to stop terrorist

activity compared to older means of conventional law enforcement. Also with the ideas and evidence presented in the paragraph focusing on governance it was made clear that the NSA lacks effective and substantial public awareness. This leaves international cooperation to be discussed. According to Andrea Mitchell and Erin McClam, of NBC News, the United States has been spying on a vast number of our known allies. The authors state that the NSA has spied on over 35 different world leaders. More specifically Mitchell and McClam talk about how the NSA had been monitoring the communications of the chancellor of German since 2002, and that recently the NSA had collected over 60 million phone calls in Spain. Both Spain and Germany are close allies of the United States. Secretly spying on one's allies is not only failing to cooperate at the current moment, but also in the future. This violation of trust creates harsh tension and feeling among nations. In the future it may be hard for the US to work with other nations because of the United States' past surveillance actions. From the evidence presented in this paragraph, and the paragraphs above, one can come to the conclusion that current NSA policy and actions fail to incorporate the idea of capacity building.

The cyberspace policy review written in 2009 was created with the intention of helping to progress how nations, specifically the US, survey in cyberspace. After examining four key ideas addressed by the cyberspace policy review, one can see that NSA spying incorporates none of these aspects. The review explicitly says that any cyberspace policy must "at a minimum" incorporate these four key points (B-5). The NSA is not abiding by documents that its own US government has written; however, this should not be the biggest concern. What should be a concern is that ever day countless numbers of people are having their privacy invaded, and their rights stripped away, for what seems like arbitrary reasons. This tally of citizens that have become victims of the NSA may seem like just a number or statistic to you, but in the future, a

future not very far away, you may become the statistic. It is time for the citizens to take a stand, and curb this self-surveillance that seems to be growing uncontrollably.

Works Cited

Bergen, Peter, and David Sternman. "Did NSA Snooping Stop 'Dozens' of Terrorist Attacks?" *CNN*. Cable News Network, 18 June 2013. Web. 25 Nov. 2013.

Fung, Brian. "We Now Know Exactly What Made the FISA Court so Upset with the NSA." *The Washington Post*. The Washington Post Company, 10 Sept. 2013. Web. 18 Nov. 2013.

Greenwald, Glenn. "Series: Glenn Greenwald on Security and Liberty: NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. The Guardian News and Media Limited, 5 June 2013. Web. 25 Nov. 2013.

Love, Dylan. "These Are Supposedly The Words That Make The NSA Think You're A Terrorist." *Business Insider*. Business Insider, 13 June 2013. Web. 22 Nov. 2013.

Macaskill, Ewen, and Gabriel Dance. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained." *The Guardian*. The Guardian News and Media Limited, 1 Nov. 2013. Web. 24 Nov. 2013.

Mitchell, Andrea, and Erin McClam. “US Coping with Furious Allies as NSA Spying Revelations Grow.” *NBC.* National Broadcasting Company, 8 Oct. 2013. Web. 25 Nov. 2013.

United States. Executive Office of the President. *Recent Changes Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. N.p., 29 May 2009. Web. 17 Nov. 2013.

United States. Government. *Administration White Paper Bulk Collection of Telephony Metadata Under Section 215 of The USA Patriot Act*. N.p., 09 Aug. 2013. Web. 17 Nov. 2013.

“Welcome to the National Security Agency.” *National Security Agency.* Central Security Service, 15 June 2009. Web. 20 Nov. 2013.