Effects on Current Day Technology, Legislation with Respect to Ethical Valuation: A Look at Edward Snowden’s Impact

Brian J. Galli, Long Island University, Brookville, USA

ABSTRACT

Edward Snowden is an American who released classified government information to journalists in June 2013. These secrets revealed the existence and purpose of numerous government mass-surveillance programs, which were developed to gather, retain, and analyze electronic information not only on a nationwide scale but also on a global scale. Due to his actions, some would describe Snowden as a villain or traitor, while others would describe him as a hero or patriot. After the release of information about large government surveillance programs, there are varied opinions as to whether this had a reforming effect on our society from a technical and legislative standpoint. However, there has been very little focus on whether the absence or presence of these changes has any correlation or effect on what we think about it ethically. This research is intended to discuss if the results of Edward Snowden’s actions had an impact on cybertechnology and legislation due to the ethical considerations surrounding it.

KEYWORDS

Computers, Cybersecurity, Ethics, Technology

INTRODUCTION

Edward Snowden is a former American government technology contractor that worked for various government agencies, such as the CIA and NSA (Greenwald, MacAskill, Poitras, 2013). In June of 2013, he released numerous classified documents that he obtained over his tenure working as a subcontractor for the two mentioned agencies. They highlighted numerous government mass-surveillance programs that were developed to gather, retain, and analyze electronic information both nationwide and globally.

Background

Snowden had a scattered education and career throughout his life. In his late teens, he was forced to take time away from high school due to a bout with mononucleosis, but he never finished (Marquis-Boire, Greenwald & Lee, 2015). Rather than fall back a year in high school, he decided to take classes at a community college and to work for a classmate who started his own technology company. Within a few years, Snowden felt deeply connected to the U.S. War on Terrorism, and in 2004, he decided to join the Army (particularly the Special Forces) (Atherson, 2014). Soon after, he was discharged due to medical issues obtained during a training accident, so he obtained a job as a
security guard at the University of Maryland’s Center for Advanced Study of Language, which is a facility used by the National Security Agency (NSA). Here, Snowden had to obtain security clearance for employment, which included a rigorous background check. Then, Snowden searched for a more stable career in the intelligence community, and he was hired directly by the CIA as a member of their “Global Communication Division” (Marquis-Boire, Greenwald & Lee, 2015). It is there that Snowden started his career in the intelligence community as an IT professional. Within a short time, he stood out amongst his peers and was chosen to attend the CIA’s “secret school for technology specialists” (Atherson, 2014). It may not be surprising to those that already know, he scored over 145 on multiple IQ tests.

In 2007, once he had completed his training, the CIA assigned Snowden to a detail in Geneva, Switzerland. It was here that Snowden began to grow concerned about practices that the government was employing its war on terror. He learned of practices that he thought were both morally compromising and illegal. At that time, he recalled wanting to become a “whistle-blower” from what he had seen, but he believed that with the upcoming changes in government (2008 presidential election), there would be a positive change in policy. In 2010, Snowden changed jobs once more and accepted a position from Dell as a sub-contractor for the NSA in Japan. Here Snowden claims to have been even more deeply disturbed by practices the U.S. government was employing around the world. Despite being troubled by the NSA’s practices, he further progressed within the organization and eventually became a trusted technologist to heads of technology for the government. Eventually, Snowden was transferred to a different NSA facility (in Hawaii), under Dell, as the lead-technologist for that location.

It is here that Snowden became familiar with many government programs of mass surveillance, which were in direct violation of the laws that governed them. Information was being sent to and from government facilities without any removal of citizens’ private details, web history, and habits. This information was being recorded and tracked, and people of Arab-American descent were being targeted without discrimination. Despite technical violations within these programs, they were not being used solely for their claimed counter-terrorism purposes. There were internal memorandums that illustrated the NSA’s purpose behind this program, which went further than counter-terrorism. Capabilities were being employed to capture compromising web activity, such as “pornography-viewing habits” and other “personal vulnerabilities” for leverage against people who had different political views than those in government (Marquis-Boire, Greenwald & Lee, 2015). Snowden noted, “It’s much like how the FBI tried to use Martin Luther King’s infidelity to talk him into killing himself,” he says. “We said those kinds of things were inappropriate back in the ’60s. Why are we doing that now? Why are we getting involved in this again?” (Gellman, 2013). Historical records of how Dr. Martin Luther King Jr. had been blackmailed by government agencies, notably the F.B.I. (Harrell, 2017), are plentiful.

Within a couple of years, Booz Allen Hamilton, a large NSA contractor, had recruited Snowden as an Infrastructure Analyst. This position was also based in Hawaii and offered Snowden an opportunity to work on both foreign and domestic projects. Here, he worked on international cyberwarfare assignments, which allowed him access to virtually all of the secret information the NSA had to offer. In doing so, he found something which he thought was the most troubling out of all the things he had seen previous to this: a project called “MonsterMind.” This was a program that would examine all internet traffic patterns coming into and going out of the United States. If a cyberattack against the U.S. was discovered, it would automatically retaliate and attack the source where it was coming from (Atherson, 2014). This was deeply disturbing to Snowden not only because of its potentially destructive nature, but also because of what that meant for the American public. Every bit of data coming in and out of the USA would have to travel through the NSA’s facilities and be examined. This meant that the government would be in complete control of the internet and have unfettered access to all data travelling in and out of the United States. Snowden thought that privacy would be gone forever, which would be a direct violation to the Fourth Amendment of the U.S. Constitution. This was what Snowden claims to have driven his decision for taking action. He had to do something about public
The Role of Organizational Culture in the Success of Changing Behaviour


[www.igi-global.com/chapter/the-role-of-organizational-culture-in-the-success-of-changing-behaviour/177622?camid=4v1a](www.igi-global.com/chapter/the-role-of-organizational-culture-in-the-success-of-changing-behaviour/177622?camid=4v1a)