Proceedings of The National Conference
On Undergraduate Research (NCUR) 2015
Eastern Washington University, Cheney, WA
April 16-18, 2015

Technology, Privacy, and Democracy

Michelle L. Stout
Political Science
Eastern Washington University
526 5th Street
Cheney, Washington 99004 USA

Faculty Advisory: Dr. Majid Sharifi

Abstract

In recent decades, advances within information communication technologies have created both challenges and opportunities to individuals and their governments, resulting in dramatic shifts in contemporary human conditions. This study explores the dimensions of these conditions. The paper is divided into three parts. The first part examines how improved technologies in personal communications are deeply linked with improved technologies of surveillance used by governments and private enterprise. Through this examination, the paper demonstrates how the linkages between the technology of communication and surveillance have created contradictory imperatives—individuals' wish for and implied right to privacy, governmental need to provide security, and capitalist institutions desire for profit. This contradiction impacts the individual's ability maintain their privacy while empowers states and corporations to increasingly violate what we had previously considered to be private. As such, the conceptual lines defining the distinction between privacy and what is public have become blurry at best, nonexistent at worst. Exploring this blurriness leads to a discussion on expanding the definition of privacy and the negative consequences of suffering from cumbersome corporate and governmental organizations that interject into people's daily lives without being responsible to the public. Finally, the third part of this paper examines the element of security but questions security in the traditional context. Focusing on what appears to be a reverse form of securitization that inhibits the public's ability to assert its democratic authority and contributes to atmosphere that protects monitoring, tracking, and data collection by powerful public and private bodies at the expense of democracy.

Keywords: Technology, Privacy, Democracy

1. Introduction

Many believe that technology in communications has indisputably improved the human condition. The modern world has become a fast moving landscape for continued beneficial advancements in communication. It is also a territory littered with potential landmines that affect the individuals' right to defend their privacy from private and governmental systems. The purpose of this research is to examine how advances in communication technologies have increased the power of governmental and private institutions to monitor activities of private citizens. The extant literature shows a contradiction between privacy rights and security needs. Of course, invoking the idea of privacy demands a working definition of what it is, distinguishing what might be considered, private or public; furthermore, the question of privacy versus security implicates the very notion of democracy. This begs the question of whether a democratic system can thrive, let alone survive, under the increasing pressure of a security and surveillance state. Relatedly, can democracy thrive under conditions of decreasing the rights to privacy? I propose that continued unregulated, unchecked, and unaccountable monitoring of society will deteriorate the concept of democracy resulting in a surveillance state that negatively impacts the human condition.

The concept of privacy and its relevance to human expression, communication, and correspondence in one form or another is not new. This basic right is now frequently challenged by recent advancement in communication

technologies as well as the expansion of the state's need to securitize spaces or issues previously not under the purview of the state. These unchecked, unaccountable, and unprecedented scrutiny practices by both governmental and private agencies have created new conditions. Concerns of how information is collected, how constitutional rights are affected, the future ramifications of data collection, and the question of ethics come into play. The role of security under the conceptual tradition of the social contract implies that individuals consent to the state's monopoly of the use of violence. As result, society depends on the capacity of the state to provide safety and security. But at what cost? In recent decades, advancements in communication technology have played an integral part in providing information to governmental authorities to better equip them with power to monitor citizens. If privacy is a cornerstone to democratic principles then it may follow that the increasing surveillance that rests on the premise than and any and every one is a potential threat to democracy. The indiscriminate watching of citizens creates the potential for societal backlash and could erode the fabric of democracy. This paradoxical situation between an individual's right to privacy and the government's responsibility to ensure security creates a state of tension. If the surveillance prevents democratic rights from being exercised in a meaningful way, then that which was to be protected, i.e. democracy, is no longer present. Freedoms are foundational and are what has contributed to the success of democratic societies. [1]

2. Technology

Improved tech in personal communication is linked to improved technology of surveillance facilitated by technologies employed in Facebook, google, gps, smart phones, cookies, and third party tracking of internet use. Communications technology has vastly altered the information scene in recent years. Innovation within the field of technology and use by private citizens has skyrocketed in an incredibly short amount of time. According to the Pew Research Center in January 2014, 90% of Americans possess a cell phone, of this population 58% own a smartphone.[2] It is now a world where information is instantaneous and participation in this exchange is increasingly essential. This has also led to a rise in dependency upon these tools in today's world. The evolution of information technology has made communication as mobile as the person who can slip their phone into their pocket. Smartphones in particular have created an increasingly smaller and more interconnected world. Proximity to one another is no longer a factor in communicating with the use of the phone as a tool. Smartphone technology possesses the capability for the user to send textual, graphic and audio messages to another within seconds, has the ability to readily connect to the internet, and with the inclusion of social media apps on the device, allow for one to interact and associate with a relatively large number of people. In addition to this increase in human communication the potential for privacy concerns has risen for users of smartphones.

Many applications available for download are free, while they may not require a monetary exchange between the producer and the consumer, instead, they require an exchange where the application may access a variety of information stored on the phone such as names, locations, pictures, contacts, and other personal information. This intrusiveness has led to more than half of consumers of these apps to either uninstall or make the decision against installing the app altogether.[2] Social media also poses concerns of personal information access. Facebook, the most popular of the social media sites, has a participation rate of 71% of internet users age 18 and up.[2] This platform offers a space with which individuals share an incredible amount of personal information. Names, birthdates, place of residence, friends, place of employment, employment history, education, phone numbers, favorite movies, authors, and activities, pictures, thoughts, and milestones are recorded in varying degrees for public viewing. This is information willingly entered by the participants, but they are not just sharing this information with their friends and acquaintances. This data is also acquired by third parties who have an interest in the information. Big data has become a billion dollar industry for private business, and the United States Government is collecting it as well.

The extent of this gathering of information has created a great deal of controversy. Edward Snowden, a former National Security Agency (NSA) contractor, leaked a sizable amount of classified information to the media in 2013 detailing just how much data the United States government was collecting on U.S citizens. This data is being collected in bulk, sifted through by data processing software, and stored for however long the government chooses to keep it. Data farms, such as the 1.2 billion dollar facility in Bluffdale, Utah, are erected to contain this information on servers, to the tune of $20 million in annual maintenance costs.[2] While those in the government state that the NSA is not listening to your phone calls, there are those in the security field who contend that metadata equals surveillance data, and can be used to track trends, habits, and personal interests.[3]

3. Privacy

Historically the conceptualization of privacy is fundamental to a democracy. In order for society to function under this specific form of government it requires that the government to a wide degree is not involved in the personal lives of its citizens. In early America, when the British began increasing taxes and restricting imports, one of the central issues for the colonists was the abuse of power by the British in the form of general warrants and writs of assistance. These legal documents gave incredible power to the person in possession of them. Under British law, the possessor had the capacity to legally enter and search any residence or building without any evidence to support justification of the searches. In addition, the general warrants and writs of assistance could be transferred to another individual and were not subject to expiry until six months after the King's death. This conflict between the early American colonist and Britain is significant as it contributed heavily to the 4th Amendment (1791) of the Constitution of the United States of America that states: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probably cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[5]

This amendment provided protection of the people from the searches and seizures that were endured while under British rule. Government authorities must follow and comply with the law of providing sufficient evidence with which to obtain judicial approval for a warrant that specifically states the people, places, and things to be searched or seized. U.S Supreme court cases such as Katz v. United States and Griswold v. Connecticut it has been determined that while there may not be an explicit right to privacy there is an implied right to privacy granted under the United States Constitution to citizens.[6&7] The issue of privacy has not been resolved here though, and continues to be challenged regularly. It is often problematic to even provide a definition of privacy with which to best describe the concept. This difficulty further hampers the cause of keeping what is private, private.

The concerns that surround the definitive characteristics of what is privacy are addressed by Daniel J. Solove, Research Professor of Law at the George Washington University Law School and author of *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, who studied the subject extensively. He contends that the two general analogies of violations of privacy, that of an Orwellian society of Big Brother always watching as portrayed in George Orwell's *1984* and the instance of a Kafka-esk world where information of citizens is used in a manner inconsistent with rule of law such as Franz Kafka's protagonist is subject to in *The Trial*, are narrowed perspectives. The primary focus of the Orwellian society is surveillance while the Kafka-esk view concentrates on the processing of information. In response to these narrow perspectives, Solove puts forth the argument that privacy is varied and diverse, requiring a more in-depth analysis of its components. This provides that the subject is one that displays an interconnectedness of individual categories under a broad topic. What he refers to as his taxonomy of privacy consists of four general categories of problems within the discussion of privacy and sixteen subcategories, situated as the following: Information with the subcategories of surveillance and interrogation, information processing with the subcategories of aggregation, identification, insecurity, secondary use, and exclusion, information dissemination with the subcategories of breach of confidentiality and disclosure, and the final category of increased accessibility with the subcategories of blackmail, appropriation, distortion, invasion, intrusion, and decisional interference.[8] The complexity within privacy contributes to the murkiness and difficulty of a concrete explanation of what it is. This demonstrates the limitations and inability to provide a clear and concise description of the concept. Under this taxonomy, Solove's goal is to: Shift away from the rather vague label of "privacy" in order to prevent distinct harms and problems from being conflated or not recognized…with no satisfactory set of necessary or sufficient conditions to define privacy, there is no one specific criterion for inclusion or exclusion under the rubric of "privacy".[8]

One of the issues under the governmental collection of surveillance is with the secondary use of the data that is collected.[8] The general public does not know how long this information will be stored, how it may be used, and what it might be used for in the future. This knowledge about citizens and the potential for future use in a manner that is not consistent with a citizen giving consent, provides the government with an incredible amount of power over its citizens and potential for abuse. The British newspaper The Guardian, reported in 2014 that Her Majesty's Revenue and Customs, proposed the selling of taxpayers data that they claim had been anonymized.[9] In the article *Thanks to Care.data, Your Secrets are No Longer Safe with your GP* by journalist Asher Wolf, she reports that "the UK government is selling off the rights to your personal health data in the name of 'transparency' and 'open data'".[9] This is further complicated with security concerns that data could be compiled that eventually identifies an individual. The effects of re-identifying personal information that belongs to the original person could have disastrous effects for the individual. If personal information is bought and sold to private companies then it presents many concerns such as who has this information, how might it be used, will it be sold again, who might be buying it, and so on and so forth.

A face to go with that information is now available. Biometrics, as stated by Katrin Laas-Mikko and Margit Sutrop, authors of *How Do Violations of Privacy and Moral Autonomy Threaten the Basis of Our Democracy*, are profiles where: Measurements form the set of the data that are 'mined' to detect the unique patterns for a particular person. Behavior biometrics is the result of profiling, in which a certain kind of image is created and attached to the person, and then matched against data that can be used to provide more complete profiles.[10]

U.S. News & World Report published an article stating that the Federal Bureau of Investigation (FBI) may gain access to biometric data from Facebook by accessing pictures uploaded to the site from users, to expand their Next Generation Identification system that will be used in conjunction with employment background checks. Regardless of whether or not one has a criminal record, the FBI could have a record of unique identifying physical characteristics of individuals.[11] The Washington Post reports that thirty-seven states utilize facial recognition from data pulled from individuals' driver's license photographs with 26 of those states allowing law enforcement to use that information.[12]

4. Surveillance

Civilization has been afforded quicker and more efficient ways with which to process and transfer information. This has improved many areas of life such as healthcare and education. Digital health records have improved efficiency in some aspects of patient care and remote learning using technology has expanded the availability of an education to those who may have been excluded prior. It has also created a world where there is a digital record of citizens within the virtual world that holds ramifications in the real world. Communication technologies' continued improvement and subsequent increase in use presents concern for misuse and abuse at a level that society has never had to address before. Often, these infringements are not addressed until after they have impacted society. Prior to September 11th, 2001 the dissemination and tracking of information was considerably less than what it is now. Neil M. Richards, Professor of Law at Washington University and author of *The Danger of Surveillance*, states that "the general principle under which American law operates is that surveillance is legal unless forbidden".[13] This principle is problematic however in contrast to the 4th amendment of the U.S. Constitution as the gathering of personal information could be considered a search and seizure under some conditions. The Presidents Review Group, which compiled the report Liberty and Security in a Changing World concluded "that some of the authorities that were expanded or created in the aftermath of September 11 unduly sacrifice fundamental interests in individual liberty, personal privacy, and democratic governance.[14] In addition, governmental institutions are not the only entities with interest in access to personal data.

The private data industry that focuses on tracking, buying, and selling personal information is a billion dollar business that is largely unregulated. The premise that it is acceptable to gather private and personal information because "I don't have anything to hide" is frequently used to protect this system of trespass against society. This widely used justification has created an environment that those subjected to the surveillance become willing participants in the reduction of their right to privacy. As it is explained in the *Protecting Human Health and Security in Digital Europe: How to deal with the "Privacy Paradox"?* by Isabell Bu'schel et al that citizens are concerned about the data mining and processing by governmental authorities and private businesses in reference to how these actions affect their autonomy and freedoms yet they willingly reveal personal information on social media sites.[15] These two elements contradict each other and in doing so enables entities that monitor individuals' information easy access to that data. Richards explains that this monitoring:

Has often been done in the name of counter-terrorism, but it has also been justified as protecting cybersecurity, intellectual property, children from predators, and a seemingly ever-growing list of other concerns. Some of the most well-known and valuable publicly traded corporations have also got in on the act, often with the consent (in varying degrees) of their customers. Surveillance, it seems, is not just good politics, but also good business.[13] By following the line of reasoning that one does not have anything to hide, it implies that one who wishes for privacy is doing something wrong. This creates a juxtaposition that the want for privacy is associated with something negative or criminal. It undermines any other part to the issue in it through this reasoning. By only addressing the dimension of the subject that states if one seeks to keep information private then they must be doing something bad, this argument fails to address any of the other issues within the taxonomy of privacy.[8]

There are ramifications to the monitoring of citizens regardless of whether one subscribes to the above argument. In the study of surveillance it has been found that one of the most effective ways to control a society is by the action of watching them. The British philosopher Jeremy Bentham's Panopticon theory is evidence that instituting an unseen watcher over people produces changes in behavior. Individuals unsure if they are being observed forces them to regulate themselves in accordance with the expectations of the watcher.[16] Both Richards and Solove note the chilling effect that surveillance produces. The idea is that the potential for scrutiny and possible negative consequences that

may result from actions produce an effect where individuals change their behavior, actions, speech, and thought to conform to the desired characteristics of those with power over the watched. [13] The result being a loss in freedom from other behaviors, actions, speech and thought. Solove states that the chilling effect is derived from issues within the privacy taxonomy under the subcategory of information processing and these effects change behaviors and interactions of individuals within institutions that have influence on the individuals' life.[8] Richards argues that the normalization of behavior and actions by way of surveillance, particularly puts intellectual freedom at risk with the absence of shields to protect privacy under extensive monitoring, thus democratic values such as those in the 1st Amendment are jeopardized.[13] If one is fearful of negative consequences from questioning or challenging the norms dictated as acceptable then we have just entered an area that incapacitates an individual from exercising their ability to remain autonomous. Society values privacy and as Laas-Mikko and Sutrop, point out theory has "indicated that the primary task of privacy with respect to the individual is to protect his or her autonomy".[10] This ability to self-govern gives the individual the capacity to make independent decisions according to his or her ideals.

The ability of private industry to gather informational content further hampers the individual's right to self-determination as well. While we like to think of the internet as free and open, the reality is that it comes at the price of the end users data. The use of tracking software on the web has produced digital profiles of individual users with detailed data markers that capture a huge amount of personal information that is traded, bought, and sold. Multibillion dollar corporations have been built off this platform which uses surveillance in marketing to influence consumers. Companies such as Amazon, Facebook, and Google use affinity data, which can be described as information gathered in which people express their likes and preferences that can in turn be used to individualize marketing suggestions to individuals.[17] Public institutions, such as education, are also being targeted by private businesses seeking data collection on society's most vulnerable citizens. When educators use providers of technology for educational purposes, the United States Department of Education in their Protecting Student Privacy When Using Online Educational Services FAQ report states that: On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party.[18] While the U.S. Department of Education claims that this data is supposed to be stripped of identifying information prior to further action with the data "for different purposes than those for which the information was shared"[18], how is that the information could be used to market directly to an individual student? Furthermore, students are generally a captive audience and exposure to marketing such as this raises ethical questions, as the intention of marketing is to influence a purchaser's decision. Self-determination is thereby impacted with exposure and in the case of a captive audience, possible repeated exposure.

5. Security

Providing security is one of the primary functions of the state. Adequate strength and capacity must be met in order for the state to fulfill this obligation. Society is dependent on the government to assure security of economic, political, public, and private institutions. Inability to meet the needs of these institutions weakens the civilization. In a democracy national security is also dependent on the society's permission of the extent that security functions can interject themselves into the society. Balance between governmental authority regarding security and the rights of the people in order to remain autonomous must be recognized.[19]

Tara McCormack, author of *Power and Agency in the Human Security Framework*, argues that in regards to international powers that security is used in a manner where inequalities in power are used by stronger states in order to keep weaker states less powerful, in part by intervening and regulating the affairs of those less powerful.[20] This same principle could be said of nation states and private corporations over citizens' autonomy. The argument for increasing security is manipulated by governmental authorities and businesses that perpetuates an imbalance of power in so that citizens' rights can be infringed upon, securing not the citizen, but expanding the power of government and corporations over the population.

Mass data collection by the NSA is touted as being essential in a world post 9/11 by government officials such as Keith Alexander, former director of the NSA, who testified that the NSA had thwarted somewhere around 50 terrorist plots.[21] In contrast, a study by the New American Foundation concluded that the NSA's bulk data collection has been of minimal use in deterring terrorism. Only 1.8 percent of the 225 cases they examined in their study could be attributed to having utilized information from the metadata captured in telephone communications. Rather the report showed that it has been traditional methods of investigation by law enforcement that initiated 60 percent of terrorism cases.[22] If security measures, such as the NSA, are not as effective as some claim, what is driving the use of technology in these ways? Part of it may be as David Lyon and David Murakami Wood note in *Security, Surveillance, and*

Sociological Analysis that: Political economy acts as a powerful driver of fusion between surveillance and security….as noted by analyses of post-9/11 social formations[23], the post-Cold War period saw a diversification of corporations previously reliant on the (and other national) military organizations for both purchases and research and development investment, in anticipation of a changed international order.[21] Much of the restructuring saw priorities shifted by companies….into areas of civil application for the kinds of technologies they had previously been developing for war.[23] This is at ethical odds with the purpose that security ideally demonstrates. If the goal is to provide a society with safety, inducing panic to the point of investing in technology and surveillance as a false sense of securitization, is problematic. Given that corporations have an incredible amount of political influence it would appear that they have taken advantage of "perceived insecurity and fear" [23] and have used this fear in order for private profit.

The competition within the surveillance industry has also been driving down the cost to those seeking an increased presence within it. Ashkan Soltani, currently the Chief Technologist of the Federal Trade Commission, authored the article *Soaring Surveillance*, in which he states:

Surveillance techniques have been exploding in capacity and plummeting in cost. One leaked document shows that between 2002 and 2006, it cost the NSA only about $140 million to gather phone records for 300 million Americans…a minuscule portion of the NSA's $10 billion annual budget.[22] It would make sense that continued reduction in cost frees up money to be spent elsewhere and increase NSA programs. Soltani offers that in order to protect society from the reduction in what he labels "natural" boundaries, i.e. technological and financial barriers, necessitates revision of the laws set up to protect privacy rights.[24] Currently, the FBI has the capacity under expanded power afforded through the PATRIOT Act that gives Special Agents the privilege of issuing National Security Letters in order to gather information "relevant to an authorized investigation"[14] that effectively gag the recipient of disclosing the request, without judicial approval.[12] In *Liberty and Security in a Changing World*, the President's Review Group on Intelligence and Communications Technologies recommends that: National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that: (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and (2) like a subpoena, the order is reasonable in focus, scope, and breadth.[12] Whether or not this and other recommendations to secure citizens' rights to privacy will be adopted remains to be seen. Once institutions are given expanded powers they are reluctant to give them up, despite the positive effect it may have on the democratic principles.

6. Conclusion

Modern civilization through the use of information communication technologies can now participate in the exchange of information with an ease previously unknown in the not so distant past. The cost of which is up for debate. More individuals than ever possess devices with which they can share an incredible amount of material, some of which, includes personal details that one desires to keep limited. The conveniences offered by tech can be perceived as free and compliment an exercise in freedoms. Yet they are anything but with the providers of services increasingly intruding on personal data exclusive to an individual, which in many cases is given willingly, though at a price that the general public is unaware. The conceptualization of privacy is being reworked and redefined with the current state of affairs in government and business. The popular argument of I've got nothing to hide therefore I don't care who is watching needs to be addressed in a manner where the implications for reckless disregard for personal information has the ability to negatively impact future endeavors needs to be brought to light. With the prospect of entities such as the FBI having access to personally identifiable information being used in collaboration with other programs that could potentially identify an individual engaging in questionable behavior and then that information being available to prospective employers, insurance companies, or law enforcement presents a host of concerns.

New problems will continue to arise within the function of privacy and new solutions will need to be sought for privacy rights. The use of software that provides protection from the constant monitoring that is occurring is available on a limited scale through projects such as Tor, a service that focuses on protecting internet users from being tracked through a diverse user base that effectively conceals the user amongst all the other individuals using the network.[25] Declining the use of applications on smartphones that request access to information and disabling the tracking features present on them are two things individuals can do. However, more needs to be done on a large scale. The speed at which these technologies develop places them in a position where society is in the position of playing catchup in order to deal with the effects of the products and services that being driven by economic factors. As Daniel Sarewitz, Professor of Science and Society for Arizona State University and author of Defending Democracy states "the time to start thinking about the impact of security technologies on democratic rights is during R&D".[26] More review and revision of government agencies, such as the NSA, that undermine democratic principles needs to be done.

Surveillance programing that provides privacy protections such as ThinThread which journalist Jane Mayer with The New Yorker reported as capable of protecting American identities.[27] Continued discussion and questioning of practices that claim to provide for the people—such as security, needs to continue within society. If security of democracy is truly at the heart of this all then the current system needs improved upon significantly in order to maintain citizens' privacy, autonomy, and the ability to exercise democratic ideals.

7. References

1. Tocqueville. (2012). *US Foreign Policy.* New York: Oxford University Press.
2. (2014). *Mobile Technology Fact Sheet.* Pew Research Center.
3. Berkes, H. (2013, September 23). Booting Up: New NSA Data Farm Takes Root in Utah. *National Public Radio*.
4. Schneier, B. (2014). Metadata=Surveillance. *Security & Privacy, IEEE, Vol. 12*(2), 84.
5. *IV., U.S. CONST. amend.* (1791)
6. Katz v. United States, 389 U.S. 347 (1967)
7. Griswold v. Connecticut, 381 U.S. 479 (1965)
8. Solove, D. J. (2007). "I've Got Nothing To Hide" and Other Misunderstandings of Privacy. *San Diego Law Review, 44*, 745-771.
9. Wolf, A. (2014, Febuary 14). Thanks to Care.data, your secrets are no longer safe with your GP. *Wired.co.uk*. Retrieved from http://www.wired.co.uk/news/archive/2014-02/04/care-data-nhs-healthcare
10. Laas-Mikko, K., & Sutrop, M. (2012). How Do Violations of Privacy and Moral Autonomy Threaten the Basis of our Democracy. *Trames, Vol. 16(4)*, 369-381.
11. Risen, T. (2014, June 8). Could the FBI See Your Selfies? *U.S. News & World Report*. Retrieved from http://www.usnews.com/news/articles/2014/07/08/fbi-may-seek-facebook-data-for-facial-recognition
12. Timberg, C., & Nakashim, E. (2013, June 16). State photo-ID databases become troves for police. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/ technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html
13. Richards, N. M. (2013). The Danger of Surveillance. *Harvard Law Review, Vol. 126(7)*, 1934-1965.
14. Technologies, P. R. (2013). *Liberty and Security in a Changing World.*
15. Bu'schel, I., Mehdi, R., Cammilleri, A., Marzouki, Y., & Elger, B. (2014). Protecting Human Health and Security in Digitial Europe: How to Deal with the "Privacy Paradox"? *Science and Engineering Ethics, Vol. 20*(3), 639-658.
16. Kietzmann, J., & Angell, I. (2010). Panopticon Revisited. *Communications of the ACM, Vol. 53*(6), 135-139.
17. Elliott, N. (2013, August 21). Google vs. Facebook in the Battle of Affinity. *All Things D*.
18. Center, P. T. (2014). *Protecting Student Privacy While Using Online Educational Services.* U.S Department of Education
19. Mill, J. S. (1863). *On Liberty.* Boston: H.O. Houghton. Retrieved from https://archive.org/details/onliberty05millgoog
20. McCormack, T. (2008). Power and agency in the human security framework. *Cambridge Review of International Affairs, Vol. 21*(1), 113-126.
21. Nelson, S. (2013, June 18). NSA Director: Surveillance Stopped 50 Terror Plots. *U.S. News and World Report*. Retrieved from http://www.usnews.com/news/newsgram/articles/2013/06/18/nsa-director-surveillance-stopped-50-terror-plots
22. Berge, P., Sterman, D., Schneider, E., & Cahall, B. (2014). *Do NSA's Bulk Suveillance Programs Stop Terrorists?* New America Foundation.
23. Lyon, D., & Wood, D. M. (2012). Security, Surveillance, and Sociological Analysis. *Canadian Review of Sociology, Vol. 49*(4), 317-327.
24. Soltani, A. (2013). Soaring Surveillance. *Technology Review, Vol. 116(5)*, 10-12.
25. Tor. (2015). *Tor: Overview.* torproject. Retrieved from https://www.torproject.org/about/overview.html.en
26. Sarewitz, D. (2010). World view: Defending Democracy. *Nature, Vol. 465*, 546.
27. Mayer, J. (2011, May 23). The Secret Sharer. *The New Yorker*. Retrieved from http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer