Panopticon in the 21st Century

Myeongsub Lee, Walter Hufstetler, Sanguk Park, Sudip Chakraborty
Department of Computer Science, Valdosta State University
1500 N. Patterson Street, Valdosta, GA 31698, USA
{mylee, wahufstetler, sanpark, schakraborty}@valdosta.edu

ABSTRACT
Surveillance has been considered an effective technique for detection and deterrence of wrongdoings by rogue entities in our society. However, the mechanism comes with a price – reduced level of privacy and trust. It also raises ethical issues regarding its deployment and use. In this paper, we present the impact of surveillance on modern society and its ethicality in the light of known ethical theories. This leads to our main discussion about the tradeoff between safety through surveillance and sacrificing people's privacy, with a focus on ethics of using such techniques. In these contexts, we consider both private and public surveillance, highlighting ethicality of use of surveillance by the government.

General Terms
Security, Human Factors, Legal Aspects

Keywords
Surveillance, Ethics, Society, Government, Impact

1. INTRODUCTION
Imagine a prison that allowed the guards to see the prisoners but did not allow the prisoners to see the guards; a giant circle of cells and a watch tower in the center. The prison design is called *Panopticon* and it is one of the few architectural designs in history to cause an ethical dilemma. The design was criticized for being inhumane, oppressive, and potentially causing psychological harm. Although the comparison between Panopticon and modern surveillance techniques may be extreme, the comparison is frequently made. From security cameras to wiretapping, almost all forms of surveillance are one-sided; and although many people feel negatively about surveillance, is their negativity justified? Before we delve in that question, let us briefly present the notion of surveillance using modern computing technology.

1.1 Surveillance and its Benefits
Surveillance is defined as "close observation" (or, monitoring) of the behavior, activities, or other information of a group or an individual, for the purpose of influencing, managing, directing, or protecting them. [10]. This monitoring can take 'human form' (prison guards, neighborhood watch, etc.) or, can be done using variety of technologies including wiretapping, security cameras, and sensors. Often these technologies are combined with other technologies like face recognition technique, pattern matching, artificial intelligence, and biometric. Surveillance serves two main purposes – one is to catch people committing crimes and the second is to deter people from committing crime. A study, done by Northwestern University over two years in Chicago, on effectiveness of security cameras to prevent crime found average 31% decrease in crime in the areas deployed with security cameras. A similar study done by Chicago Police Department found 14% decrease in crime in specific areas with security cameras. From the findings of these studies it can be concluded that surveillance have a statistically significant positive impact on the prevention of crime [1]. Surveillance cameras combined with other technologies, for example, facial recognition revealed similar result. The NYPD has made more than 1,000 arrests using the technology. They also routinely use facial recognition technique to spot fake driver's licenses [2]. One of the significant successes of surveillance (through security cameras) is identification of two terrorist brothers responsible for Boston Marathon bombing in 2013. Surveillance cameras worn by law enforcement officers ("body cam") help in documenting incidents with them or bring unjust officers to attention/justice.

1.2 Surveillance and its Criticisms
Despite its benefits, surveillance is not criticism-free. Great number of people feel negatively about surveillance, especially when it is deployed by a government. The main concern is reduction of privacy, and as the growth of technology expands and accelerates, privacy and surveillance will only become a more important conversation. People often willingly relax their privacy perimeters (for example, postings on social networking sites like Facebook, Instagram etc.), but do not feel comfortable to relax the same when it comes to surveillance as it allows in diminution of privacy covertly. A recent example is Google Glasses; they were banned from many establishments because they allowed people to take pictures and record videos discreetly. In fact, surveillance systems could be abused as criminal abuse, institutional abuse, personal abuse, discriminatory targeting, and voyeurism. The lack of limits and controls on use of the installed cameras adds to the above issues. These limitations of surveillance force us to consider the ethics of the notion. Careful examination of ethicality of surveillance is more relevant when the technique is deployed by trusted entities like employers and government.

1.3 Contribution and Roadmap
In this paper, we discuss the last issue mentioned in the previous subsection. Our objective is to highlight the potential harms of surveillance, especially its significance when done by government. We present examples of known cases of surveillance and discuss

their impacts. We also present a discussion on ethical issues concerning surveillance.

The rest of the paper is organized as follows: Section 2 presents some background discussions on ethical theories. In Section 3 we discuss impact and ethical concerns related to surveillance by private organizations and the government. We enumerate potential harms of surveillance in Section 4 and discuss ethical concerns related to specific harms. We briefly present avoidance of surveillance using anonymity in Section 5. Finally, Section 6 concludes the paper.

2. BACKGROUND ON ETHICS

In this paper, we discuss ethics of surveillance and for that purpose will refer to some of the existing ethical theories. In this brief section, we present the necessary background information regarding ethics. We first present three definitions that are related.

*Definition 1: A **society** is an association of people organized under system of rules designed to advance the good of its members over time.* [17]

*Definition 2: **Morality** is a society's rules of conduct describing what people ought and ought not to do in various situations.* [18]

*Definition 3: **Ethics** is the philosophical study of morality – a rational examination into people's moral beliefs and behavior.* [18]

From the definition, we observe that while the notion of morality may vary from society to society, ethics is more objective, being a rational, systematic examination of the guiding rules of morality. Nonetheless, the examination itself may vary based on its underlying principles and procedures. Scholars (including thinkers, philosophers, sociologists etc.) have proposed many ethical theories for this purpose. Some of them are widely adoptable and some are very restrictive. These theories are categorized into two broad groups – workable and non-workable.

*Definition 4: A **workable ethical theory** is systematic analysis that is capable of producing explanations, using logical reasoning based on facts and commonly held values, that might be persuasive to an audience open to rational arguments*.

In this article, we refer to only workable ethical theories. Especially, our discussions are based on three workable ethical theories – *Kantianism, Utilitarianism,* and *Virtue ethics*.

Kantianism is based on two categorical imperatives that are unconditional rules applicable regardless of circumstances. The first imperative basically states that people should act only on moral rules that they accept that everyone else would follow without any contradiction. The second imperative states that people should treat themselves and other people as ends and not the means to the ends.

Utilitarianism is based on *principle of utility* (sometimes called *Greatest Happiness Principle)* that measures level of right (or wrong) of any action to the extent that the action increases (or decreases) the "utility" (or, total happiness) of concerned entities.

The virtue ethics is based on virtuousness that are character traits that human beings need, to be happy and improve their lives. A person having those character traits is considered virtuous, and according to virtue ethics, a right action is that a virtuous person would do in the same circumstances.

In the next section, we attempt to answer ethical questions posed in the context of applicability of surveillance techniques. While a detail ethical analysis of surveillance in the light of workable ethical theories is not the focus of this paper, the above background information would be useful to understand the discussions presented there. In particular, it would help the readers to understand the context of terms like "ends", "means" and "virtue".

3. SURVEILLANCE IMPACTS & ETHICS

There are those with very strong opinions regarding surveillance; some say that if one is not doing anything wrong, one not need to worry about being watched, others say that surveillance of any form violates their human right to privacy. However, most would agree that the level of surveillance should be proportional to the situation at hand, and that the benefits should, even if marginally, outweigh the harm caused. For example, is it necessary for a parent to setup a state-of-the-art security system to make sure no one steals from his/her child's lemonade stand? Probably no, as it is not cost effective and may scare off customers. Would the same security system be necessary in an institution such as a bank? Probably yes, as banks are frequently targeted for robbery and the benefits of the system would most likely outweigh the harm. Therefore, based on the needs we voluntarily agree to be surveilled and willingly relax our privacy demands. For example, we "agree" to share our location information with telecommunication companies by using our cell phones. This information, collected by private organizations, can be passed to government and made public if need arise. Other than this form of "voluntary surveilled" state, private and government organizations collect and analyze data on individuals and groups through different forms of surveillance. Next, we discuss the impact and ethicality of use of surveillance by private organizations, followed by a similar discussion when the same is applied by government.

3.1 Surveillance by Private Organizations

Employers frequently use surveillance techniques to monitor their employees. An example of reasonable surveillance would be introducing a time card due to a high number of employees coming in late or missing work [4]. Monitoring the Internet activities of employees to check whether they spend the work resource (working hours, computers, network bandwidth etc.) on non-work related websites could be effective, but it would violate the worker's privacy. Employers must choose forms of surveillance that keep productivity up without making employees uncomfortable. Companies generally have precautions in place to prevent common instances of mal-intent from both employees and the public. Security cameras and alarm systems are extremely common forms of surveillance that raise very little ethical concern. Requiring employees to use a timestamp, monitoring the location of delivery trucks, and keeping a close watch on the cash register are also common surveilling methods that raise little concern, mainly due to them having such an obvious and strong benefit to the employer. Listening to employee's phone conversations, keylogging company computers, and monitoring every website the employees visit are much more concerning forms of surveillance; these techniques are generally criticized for being unethical due to their extremely invasive nature and ability to cause employees greater mental stress. Some of these surveillances, despite negative feeling about them, are arguably necessary. For example, monitoring the employees' E-mail is a big way to protect the company's important data from leaks, protect company assets, and ensure job performance. However, this monitoring is sometimes considered an invasion of privacy in the companies. Furthermore, some of the monitoring software allows the employer to enable view of computer screens, record keystrokes, check the outgoing messages on any chat program or Web-based E-mail. These surveillance activities invade on employee's privacy and with more sophisticated surveillance software, employee's privacy erodes further [14]. Table 1 summarizes, as identified in [11],

compensating factors (supporting and disapproval) of email surveillance on employees of an organization.

Table 1. Balancing Factors of Monitoring Employee's Emails

In support	Not in favor
Organization is responsible for employee's conduct	External email accounts outside the perimeter of company's resource & bound
Protect assets and resources	Employee's private interest always exists, even at work
In U.S., under ECPA[1], it is supported by law	Can reduce transparency & trust, generating stress
To direct employee effort appropriately	Legal standards vary and may not ensure desired result

3.1.1 Ethical Question

The organization has every right to employ mechanisms to protect its assets and prevent wrongdoings, but at the same time bears responsibility to create a safe and productive environment for its employees. Employers can generally be held responsible, legally, for problems that occur within the workplace; therefore, it is important for employers to know what is going on with employees. Employees harassing other employees, abusing customers and getting involved in illegal activity could harm the entire business. Most would agree that the organization should be aware of these things and have a responsibility to fix them; however, the question generally asked is, "how far should they go?" [7].

Asking whether a surveillance measure is effective is only one question that needs to be asked. After it is determined that the technique will be effective, the next question must be "is it ethical?". To determine whether it is ethical, the following questions need to be asked:

1. Are the ends good or good enough?
2. Are the means proportionate to the end?
3. Can the ends be secured in a less invasive manner?
4. Will the means secure the ends?
5. Is there something intrinsically problematic about the means?
6. Will the means have deleterious consequences that would make their use inappropriate? [8]

The above questions can be summarized into following two common ethical questions:
(i) do the benefits outweigh the harm?
(ii) Is there anything unvirtuous about the means?

3.1.2 Ethical Analysis

As mentioned before, detail analysis in the light of workable ethical theories to answer the above two questions is out of scope of this paper. Nevertheless, we present a brief analysis using a combined context. From *Kantian* perspective, the surveillance techniques and policies are the means and the users/assets and their protection are ends. They are consistent with the categorical imperatives of Kantianism, but in some cases of surveillance, the ends are used as means to reach the goal. That is, people's privacy is ignored to achieve desired level of surveillance. From *utilitarian* perspective, it is hard to justify any action if the benefits of that action do not exceed the harm that is caused by the action. In this case, often the harm in the form of people's discontent is ignored. Also, the action itself must be *virtuous*. Stealing from 100 people to feed 150 would be unvirtuous, even if the benefits of this action exceed the harm caused.

3.2 Government Surveillance

Government surveillance is the most powerful, yet potentially dangerous form of surveillance. Surveillance by the government has the potential to improve national security; on the other hand, that itself may become a national security issue, putting the citizens of a country at risk. For example, a country may believe that it is protecting the citizens by collecting their data, believing that they could potentially find domestic terrorists with the data collected. However, the consequence could be disastrous if a foreign enemy group somehow hacked into the government database and collected the data of all its citizens. It is also pertinent to observe in this context that while doing so (protecting national security) whether the government is overstepping and infringing on its citizen's privacy rights.

3.2.1 Impact of 9/11

The September 11th attacks in 2001 brought the issue of surveillance into public conversation. After the attacks, the U.S. National Security Agency (NSA), as part of the war on terror, was authorized by executive order to monitor, without search warrants, the phone calls, internet activity (this includes emails, web pages visited, online messaging and others), text messaging, and other communication involving any party believed by the NSA to be outside the U.S., even if the other end of the communication lies within the U.S. The most controversial part of his plan was that the NSA could do this, without a warrant. Americans were divided about their approval of this, with slightly more than half supporting the warrantless government surveillance according to several polls taken in 2006, several years after the attacks. Only few polls (CNN, Gallup, and USA Today) reported more Americans against the surveillance, 50% against and 47% in favor. The other 9 polls showed 2% to 13% more Americans supporting the security measures as opposed to disapproving of it [3]. If the same poll was taken before the attack, there would certainly be less support for the amped up surveillance.

3.2.2 Impact of Whistleblowing

In the cases where surveillance by government is considered, by group of citizens, as overstepping on their part, confidential information released by whistleblowers play a big role. Analysis of these details help the citizens to answer the common ethical questions posed earlier. That is, it enables people to judge the ethicality of the surveillance. The case of Edward Snowden is one of such examples that raised different levels of concerns for both groups (in favor, and against) regarding government surveillance. Edward Snowden was a Central Intelligence Agency employee who leaked classified documents revealing that the United States government had been spying on its own citizens as well as other governments around the world. The documents include a level of details and analysis that is not routinely shared with Congress or the special court that oversees surveillance. For this revelation, he was praised by large group of people for exposing government mass surveillance. However, many accused him of compromising national security by releasing important government documents. As cascading effect reports by other agencies brought out that NSA, under the surveillance program named PRISM, was collecting telephone records of millions of citizens. Telecommunication company Verizon was forced to release information about

[1] Electronic Communications Privacy Act of 1986

international calls between April and July of 2013 [9]. Under the same program, NSA tapped into the servers of big farms like Facebook, Google, Microsoft, Yahoo to track online communications. The leak created mistrust between the United States government and its citizens, as well as tension between the United States and countries that had been spied on.

3.2.3 Ethical Issues

Government has benevolent interest in keeping its citizens safe. To achieve this goal, government should receive real time data of specific things that are happening. The best way to obtain that data is by watching, tracking, or recording actions of individuals and groups. However, the rise in number of incidents harmful to the society, growing mistrust (due to activities of rogue entities), and advancement of technologies contributed to overstepping of government's boundaries regarding monitoring of the citizens. Taking all these surveillances discussed in the previous subsections into account, individuals in U.S. have barely any privacy from the government. The fear of being watched forces people to act and think differently from the way they might otherwise. A fear of loss of control over their personal lives has grown among citizens. Another risk is that surveillance can lead to domination [15], thereby creating a power dynamic between the surveilled and the entity controlling the surveillance. This disparity increases the risk of discrimination and prosecution for critics of the government. Such selective enforcement raises a serious ethical issue and would be considered unethical by most of the workable ethical theories. Another ethical concern is government's ability to force non-governmental organizations to be involved in surveillance of citizens whose interest the organizations are committed to protect.

4. SURVEILLANCE HARMS AND ETHICS

The potential harms of surveillance are vast and far reaching. Depending on the level of surveillance and type of surveillance used, the harm can be nonexistent or dangerous. Following is a list of potential problems that can arise from the use of surveillance [4]:

1. Privacy violations
2. Chilling effect
3. Social sorting: stereotyping, stigmatization, discrimination
4. Paternalism (harm to autonomy)
5. Social fatalism
6. Behavioral uniformity
7. Imbalance of distribution of costs
8. Diminution of trust
9. Vulnerability
10. Fear of control
11. Human error and abuse of power
12. Fear of being found out when hiding legitimate information

From the above list, we choose to elaborate on item 2 (Chilling effect) and item 11 (Human errors and abuse of power) due to their significance on ethical consideration of surveillance.

4.1 Chilling Effect

The chilling effect refers to the phenomenon where people are deterred from using their rights, usually free speech, due to fear of legal retaliation. Government surveillance can play big role in bringing chilling effect. After the 2013 leaks made by Edward Snowden, more Americans were concerned about government surveillance. The documents revealed that the United States government had been monitoring its citizens' phone calls and internet activity. One study found that Americans' internet search activity changed after the leaks. Among articles that contained government tracked keywords, there was a large drop in their views after the revelation. People are more likely to avoid articles if they believe the government is watching who searches for those articles. Keywords and articles in the study included "eco terrorism", "suicide attack", and "dirty bomb" [5]. In line with the chilling effect, this research shows that citizens' awareness of mass surveillance can deter them from exercising their legal rights. In this case, internet users were deterred from researching important information with benign intention about terrorism.

4.2 Human Error and Abuse of Power

As identified earlier, abuse of surveillance technology can come from the private sector and the government sector. There was one case of a school using laptop video cameras to spy on students while they are at home. The students found out about this spying after one student was disciplined for "improper behavior", the principle showed the student an image that was taken from the laptop while the student was at home. Other students and parents claimed the school had captured images of the students while undressing. However, the school maintained the position that the cameras were only to be used if the laptops were stolen or lost and apologized for any problems they had caused [12]. This situation highlights the differences of perspective that can appear when dealing with surveillance. The school believed it was necessary to have access to the cameras in case the laptops were stolen or lost, the students and parents believed the cameras were an outrageous violation of privacy.

There is also a term, LOVEINT, which refers to government intelligence agency employees using their abilities and technology access to spy on their partners. The technology and employee's skills are used to find out who their partners have been in contact with or what they have been saying or doing online. Within the NSA, although the practice is infrequent, it demonstrates the possible abuse that arises from surveilling technologies [13].

4.2.1 Ethical Concerns

There are opposing views about the ethics of parents spying on their children. Some argue that parents have that responsibility, while other people opine that children deserve just as much right to privacy as adults do. However, the issue with this is that spying on children may not reveal that they have done something wrong, but it may reveal information that they did not want you to know; something that could embarrass them. According to Professor Anita Allen, spying on children is okay, if it is done for their own good. Children generally cannot make smart decisions for their future; they generally care more about what their friends think about them. Also, children are frequent targets for predators; therefore, it is the parents' responsibility to protect them. However, she also argues that a parent monitoring their college age children would be unnecessary since college aged children are old enough to make their own decisions; nonconsenting adults are off limits for this type of surveillance [6].

5. AVOIDING SURVEILLANCE

It is true that most of the surveillances do not force citizens to release information and rather done quietly. However, discomfort felt due to the knowledge of being surveilled, people try to use different mechanisms to avoid surveillance. Here we highlight one such technique – *anonymity*. Becoming anonymous is a way of

fighting back against surveillance. Anonymity itself is ethically neutral but what someone does with anonymity can be harmful or beneficial. In one survey, it was found that 86% of Internet users have taken steps to hide their footprint online, such as email encryption and using an alias instead of their real name. The same study found that 55% of Internet users have made attempts to prevent individuals, organizations, and government agencies from spying on their internet activity. Figure 1 illustrates result of a PEW Research Center's Internet and American Life Project Omnibus Survey that identifies categories of entities on the Internet that have been avoided by people using some form of anonymizing scheme. The survey was conducted in July 2013 through landlines and cellphones on 792 English-speaking Internet and smartphone owners. The margin of error on the survey sample is +/- 3.8 percentage point [11].

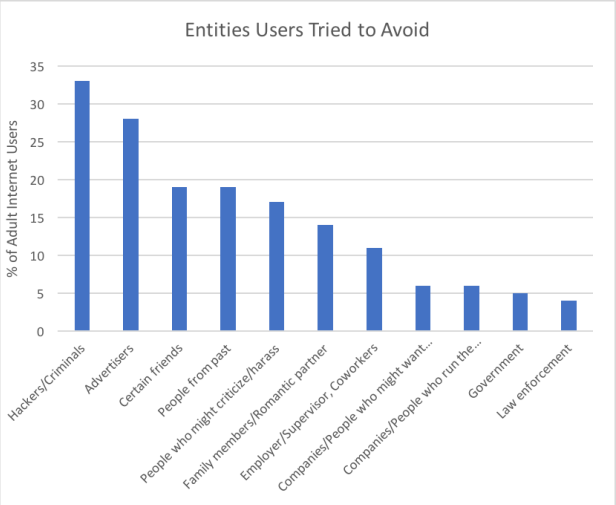

Figure 1: Distribution of objectives for anonymity

With advancement of technology, several tools/software are available for preserving privacy and anonymity. Software like TOR[2] makes computer's IP addresses almost untraceable. Figure 2, based on the data collected in the above survey [11], shows the ways the users try to achieve anonymity (or, avoid monitoring).

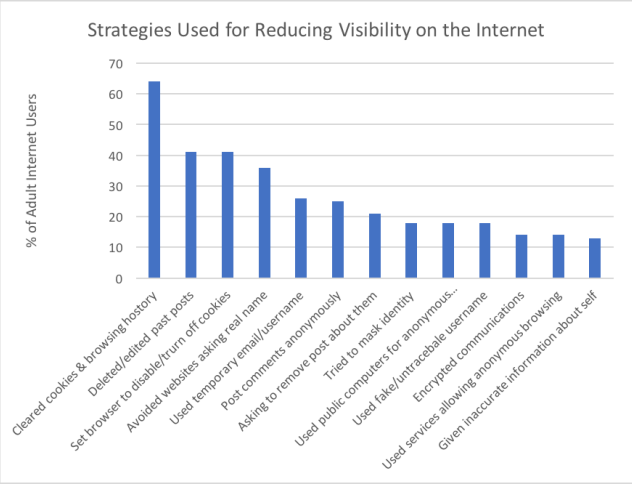

Figure 2: Strategies used to achieve anonymity

[2] The Onion Router

Nevertheless, most of the legitimate users have been found not using any such advanced privacy preserving or anonymizing software. They are rather used by group of people roaming in the "dark net" (or, dark web) with mal-intentions.

While having unnecessary and personal data collected from internet users by large corporations is not an ideal, neither is complete anonymity. Due to societal norms and laws playing a huge role in human behavior, when those rules are taken away, it can lead to disorder. One study, done in 1973, found that warriors who wore masks and body paint during tribal wars were more likely to torture and mutilate their captured prisoners. Another study using university students found that students who wore hoods or masks were more likely to administer electric shocks to their fellow students. One study done in Ireland showed that criminals who tried to disguise themselves inflicted more severe wounds in their victims [16]. This human behavior obviously does not disappear whenever people log into their computers. The criminal activities that occur on the anonymous side of the internet, the dark web, show the same type of results.

6. CONCLUSIONS

The rise of global terrorisms, a ubiquitous form of surveillance seems unavoidable to ensure safety of citizens. After September 11 terrorist attacks, U.S. government engages itself with private organizations for gathering of intelligence, thereby forming a massive surveillance industry. Since then the market for surveillance tools and software experienced a phenomenal growth from almost zero to a multibillion dollar industry in last one and half decades. Nonetheless, omnipresence of surveillance has created a debate on its effectiveness versus its disadvantages. In the grand scheme of things, people will generally be for surveillance when it benefits them and against it when it does not. However, an interesting note when dealing with internet privacy is that one's privacy concerns do not always accurately reflect their online behavior [5]. A person may feel very strongly against online government surveillance when they are doing nothing that the government would even care about. The concept of being surveilled is uncomfortable for many people, even if they are not doing anything illegal. Therefore, when exploring whether a form of surveillance is ethical or unethical, one must take into consideration several things like "does it cause harm?" and "is it justified?". The end results of surveillance do not always justify their usage, especially if the usage causes harm to the society or individuals. The comfort level of the society must be considered, as well as a benefit/cost analysis of each surveillance technology. Also, when discussing the ethics of privacy, the person's feelings must be considered. Mass surveillance tends to make the population more uncomfortable with going about the daily life, thus lowering their quality of life. Having freedom generally makes people happier. Alternatively, surveillance could also make much of the population feel safer, thus raising their quality of life. There must be a balance between freedom and safety.

7. REFERENCES

[1] Shah, R., & Braithwaite, J. 2013. Spread too thin: analyzing the effectiveness of the Chicago camera network on crime. *Police Practice & Research*, *14*(5), 415. doi:10.1080/15614263.2012.670031

[2] Fitzgerald, M. 2015. Face Tıme. *Discover*, *36*(10), 30-37.

[3] Newport, F. 2006. Where Do Americans Stand on the Wiretapping Issue?: Despite differences in question wording, it appears that Americans tilt toward favoring the program. *Gallup Poll Briefing*, 1.

[4] Macnish, K. 2015. An Eye for an Eye: Proportionality and Surveillance. *Ethical Theory & Moral Practice*, *18*(3), 529-548. doi:10.1007/s10677-014-9537-5.

[5] Penney, J. W. 2016. Chilling Effects: Online Surveilance And Wikipedia Use. *Berkeley Technology Law Journal*, *31*(1), 117-182.

[6] Allen, A. L. 2008. The virtuous spy: privacy as an ethical limit. *The Monist*,*91*(1), 3-22.

[7] Mika, K. 2014. The benefit of Adopting Comprehensive Standards of Monitoring Employee Technology Use in Workplace. *Cornell HR Review*, 1-7.

[8] Kleinig, J. 2009. The Ethical Perils of Knowledge Acquisition. *Criminal Justice Ethics*, *28*(2), 201-222.

[9] Lyon, D. 2015. The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society*, *13*(2), 139-152.

[10] Lyon, D. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press

[11] Rainie, L., Kiesler, S., Kang, R., & Madden, M. 2013. Anonymity, Privacy, and Security Online. Retrieved from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online

[12] Keizer, G. 2010. Pennsylvania schools spying on students using laptop webcams, claims lawsuit. Retrieved from http://www.computerworld.com/article/2521075/windows-pcs/pennsylvania-schools-spying-on-students-using-laptop-webcams--claims-lawsuit.html

[13] LOVEINT: When NSA officers use their spying power on love interests. (n.d.). Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/

[14] Smith, W. P., & Tabak, F. 2009. Monitoring Employee E-mails: Is There Any Room for Privacy? *Academy Of Management Perspectives*, *23*(4), 33-48. doi:10.5465/AMP.2009.45590139

[15] Barton Gellman and Matt Delong, "NSA report on privacy violations in the first quarter of 2012", Washington Post, August 15, 2013.

[16] Silke, A. 2003. Deindividuation, Anonymity, and Violence: Findings From Northern Ireland. *The Journal of Social Psychology*, 143(4), 493-499. doi:10.1080/00224540309598458

[17] Rawls, J. 1999. *A Theory of Justice*, Revised Edition. Belknap Press of Harvard University Press, Cambridge, MA.

[18] Quinn, M. 2017. *Ethics for the Information Age.* 7th Edition. Pearson Education.