***Introduction***

How would you feel if you saw someone standing outside your bedroom window, staring in through the curtains? The most common response would be to call the police. However, what do we do when the government and/or companies are monitoring and tracking us? We all just try to forget about it and go on with our lives and ignore the feeling that we are being watched. There’s no reason you have to reveal your secrets just because you want to use the internet. We use the internet for almost every aspect of our lives, it’s a way to manage our social lives, apply for jobs, seek information, and even in some cases find romance. The question is what is the government’s responsibly to not spy on their citizens and what is the company’s responsibility to not spy on their users? I will be focusing on the positive and negative consequences based on responsibility of the government and the companies. Is surveillance by the state, considered to be separate from surveillance by commercial organizations, or are they considered to be equal?

In 2016, the Journal of Applied Philosophy by Kevin Macnish stated that there is a debate over whether privacy is a matter of control or a matter of access. One side of the debate are those who are arguing that the loss of control creates a loss of privacy. While the other side feels that a loss of privacy only happens when a person’s information is accessed.

***Body***

Some positive consequences of the government being able to track us, is that it keeps people safe and it helps detect threats.

Marc Thiessen from the Washington Post argues that there are only three ways that the government can collect the data that is needed to keep everyone in the country safe. Officials can obtain the information by questioning subjects, infiltrating enemy groups, or using intelligence resources to monitor communications. The argument is that the government’s surveillance on us is essential to detect any association with international terrorism. Keeping an eye on Internet communications is key to keeping the nation safe from spies, terrorists, and kidnappers. By gathering more data, it can be argued that crime is reduced.

Some negative consequences of the government being able to track us, is that surveillance can ruin our security and hackers could gain access to the system and obtain our information.

Although the general argument is that surveillance and gathering data helps to improve security, it can also damage security and increase risks. Bruce Schneier from Data and Goliath in 2015, states that “Terrorist plots are different, mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarm that they will be useless.” He also states, “In the years after 9/11, the NSA passed to the FBI thousands of tips per month, every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obliged to investigate all the tips.” These comments open the question of whether the data collection helps security from terrorism and other dangers. Data collected about regular citizens could be used against them or to obtain an unfair advantage. In 2016, the journal of Cyber Policy by Paul Bernal states that “the idea of ‘tightening’ security actually improves security is one that should not be taken at face value.”

Hackers could potentially gain access to the databases of the government surveillance programs and sell it to rival governments, companies or organized crime groups. Many Americans search the internet for products and to make purchases on a daily basis. This gives hackers the opportunity to target and attack them. In 2017, by the journal of Computers in Human Behavior, Tracy Hong states that “The reported financial loss of Internet scams was more than $800 million in 2014.”

Some negative consequences of companies being able to track us, is that they have made their users dependent on their services and they don’t even know they are being monitored.

Internet Services such as, Google, Apple, YouTube, and other online services stated that the government has forced them to pass on records about users. The internet is a necessary part of people’s life all around the world. Apple, Amazon, Google, Microsoft, and Facebook are dominating almost all online services. Google now controls 90% of search engines. The companies have made people dependent on their services and they now monitor every message and search made.

When you grant an app access to your camera and microphone, they now have access to both your front and your back cameras. This is apps like Facebook, Snapchat, Instagram, Twitter, etc. They can record you at any time the app is in the foreground and even take pictures without you knowing. Facebook and Google’s surveillance of people around the world threatens human rights.

Alexa is supplied with a microphone that is always on. It is quietly listening for a wake word like “Alexa.” These devices are now living in our living rooms and kitchens, and on our bedside tables, or even in our pockets. According to the Personal and Ubiquitous Computing journal, in 2018, by William Palmer, “There has been a total of 8.2 million Echo family devices sold since 2014, and Amazon controls 70% of the market.” AVS also known as The Alexa Control System provides voice control services for the Amazon Echo. Alexa Voice Service can power any computing device connected to the internet that has a microphone and speaker. Amazon keeps a copy of everything that Alexa is activated with the wake word. There needs to be a solution for users to have the confidence that bringing these devices into their homes will not interfere with their privacy. One major concern is that the Echo could be configured to record every word said in a home. The biggest threat to our privacy is not that Alexa may overhear a crime, it is that law enforcement will use such devices in new ways that users are not prepared for during investigations. There have been judges that issue warrants for Alexa’s recordings.

Siri is also supplied with a microphone that is always on. It is quietly listening for a wake word like “Hey Siri.” Apple also keeps recordings of your interactions with Siri to help train their artificial intelligences. In 2016, the journal of Forensic Sciences by Graeme Horsman stated Siri could be set up to permit interactions even when the device is locked.” This can cause an even bigger issue because if your iPhone mistakenly hears “Hey Siri” when you say “They seriously,” you just interacted with a third party, and now they have a record of your conversation transmitted and saved.

In 2013, by the journal of Science and Engineering Ethics, Stephanie Bird states “that security and privacy are at opposing ends of a continuum along which a balance point can and should be found, that is, that there is a theoretical point at which ‘‘enough security’’ can be balanced against ‘‘enough privacy’’

In conclusion, the issue of government and company’s surveillance on their users is unacceptable. Even though there are some benefits of surveillance on the internet, the surveillance leaves far too much power in their hands.

b

Bernal, Paul. “Data gathering, surveillance and human rights: recasting the debate.” *Journal of*

*Cyber Policy*, vol.1, no. 2, 2016, pp. 243-264

Bird, Stephanie. “Security and Privacy: Why Privacy Matters” *Science and Engineering Ethics,*

vol. 19, no. 3, 2013, pp. 669-671

Chen, Honglian. Beaudoin, Christopher. Hong, Tracy. “Securing online privacy” *Computers in*

*Human Behavior*, vol. 70, 2017, pp. 291-302

Ford, Marcia. Palmer, William. “Alexa, are you listening to me? An analysis of Alexa voice

service network traffic.” *Personal and Ubiquitous Computing,* vol. 23, no. 1, 2018, pp. 67-79

Horsman, Graeme. “Loose-lipped mobile device intelligent personal assistants: A discussion of

information gleaned from Siri on locked iOS.” *Forensic Sciences,* vol. 64, no. 1, 2019, pp.

231-235

Macnish, Kevin. “Government surveillance and why defining privacy matters in a post-snowden

world.” *Journal of Applied Philosophy,* vol. 35, no. 2, 2016, pp. 205-464

Thiessen, Marc A. “Marc Thiessen: How Obama's IRS Scandal Harms National Security.” *The Washington Post*, WP Company, 5 Aug. 2013, [www.washingtonpost.com/opinions/marc-thiessen-how-obamas-irs-scandal-harms-national-security/2013/08/05/9fea9616-fde1-11e2-96a8-d3b921c0924a\_story.html](http://www.washingtonpost.com/opinions/marc-thiessen-how-obamas-irs-scandal-harms-national-security/2013/08/05/9fea9616-fde1-11e2-96a8-d3b921c0924a_story.html)