Government Monitoring: Are We Really Being Watched?

Christopher Griste

Abby Heidelbaugh

Bethany Nehring

Jordana Oman

Salisbury University

Author’s Notes:

CMAT 297-002

Professor Chrys Egan

Spring 2019

Contact: cnegan@salisbury.edu

**Abstract**

The purpose of this study was to better understand the methods and extent of technological monitoring that the national government and other national security agencies utilize in their daily operations. Data was gathered by examining pertinent research of professionals within the field and a survey distribution. Subject selection for the original *Government Monitoring Survey* was restricted to undergraduate students currently attending Salisbury University. The research professor sent the Consent and Disclosure forms with the survey link to the “all student” email list. No personal identifiers were attached to the information gathered. Efforts were made to have a stable data sample of the four primary undergraduate student statuses (Freshman, Sophomore, Junior, Senior) to adequately represent the undergraduate student population. All subjects of this study were at least 18 years of age. Results from the surveys showed that students believe the United States Government is monitoring what they search. While they are aware that agencies such as the National Security Agency are doing this, they understand that it is for their safety.

**Introduction**

Background

 In today’s society, government monitoring has been an increasing issue and it is done by devices used in day to day lives such as cell phones and laptops. This can also be done through apps such as Facebook, Instagram, and location services. Stingrays are devices that can pinpoint a phone’s location and record the number that is being called, which the government has two ways of doing. These are invasive cell phone surveillance devises that mimic cell phone towers and send out signals to trick call phones in that specific area into transmitting their locations and identifying information, according to aclu.org. Technology has made an impact on society, but society does not necessarily know what happens inside their devices. Cell phones are the primary way of how people stay in touch with one another and are used for hours at a time. Phones and laptops are also used for work, games, and anything you can think of. It is no surprise that the government could be tracking people through technology

Rationale

 This study delved into the idea that the government is watching society’s every move. Through the use of surveys that was administered to different undergraduate students from Freshmen to Senior year at Salisbury University, researchers were able to get an idea of how aware people are to the government monitoring society. This research attempted to find out if society is really being watched, especially through cell phones and personal computers. This study is significant because it brings out the truth of how the government may monitor citizens’ everyday devices. Currently, the invasion of privacy is at an all-time high on account of the increased technological advancements.

**Review of Literature**

 Some people may consider the government’s current data collection process as a violation of human rights and privacy. However the government agents that are currently collecting data disagree; they think that government surveillance is a primary function of the way the United States national government operates. Additionally, the data they collect is only analyzed by private corporations that are required by law to keep recovered data confidential (Dourish, P. 2014). At that point there is a question that people ask themselves: would data collection stop even if the public wanted it to? One of the things government data collectors analyze the amount of interactions a person has with a computer, not necessarily the specifics of what an external user is searching.

 The implications of having many differently coded interactions with computers, for example, having a separate mouse, keyboard, and monitor are all used to complete one interaction such as clicking the link to a website or opening a file. This means that individuals are interacting more and more with monitors and the path our mouse takes to get from one end of the screen to another is tracked and recorded. Different interactions include, but are not limited to the links that lead to other pages, what the mouse hovers over for a longer duration than the rest of the screen, and likewise what users may find interesting. All of that is recorded to be later analyzed by government specialists. However there are certain defaults such as predictive text and auto-correct that may change the meaning of the context of a specific message. If the context is changed, a red flag may pop up in the data collection process and that may change the outcome of that particular message when in reality the initial context was different, harmless even (Dourish, P. 2014).

 At one point in the 1990’s, the United States government was worried that people were making a machine that can pick up and interpret radio waves that travel around us (Soghoian, C., & Pell, S. K. 2014). In effort to stop the average citizen from producing such a machine, the government passed a law banning them. And yet it is after 2010 and now the government has access to those very same machines they made a law against. There is a public outcry that this should not be allowed. However, because of the training that government analysis agents possess, they are meant to look for specific information. With this being the case, the government has determined that its agents are not using these machines maliciously; their purpose is solely to look for threats to national security.

 In addition to tracking movement through the internet, the government has access to a lot of the information stored in social media platforms such as Facebook, Twitter, and internet browsers. The United States government even has access to what users search if they are outside of the country (Penny, L. July 3 2014). The reason for that is because those sites are based in the United States and therefore must comply with national surveillance laws (Penny, L. July 3 2014). However, government officials are more so concerned with data that could suggest a threat to national or international security. They are trained to skim over anything that is not flagged as dangerous, and more often than not they do not read or analyze personal information unless it would provide a breach in national security. That means that they skim over personal notes and “love letters” if they even look at it at all.

 Finally, in order to completely understand the issues at hand, a critical analysis of the issue and the context of a given situation is necessary (Dourish, P. 2014). In this analysis, one can truly understand all of the different possible contexts and how messages and meanings may be changed in a context different from the original one. Edward Snowden, who in 2013 was responsible for the breach in surveillance confidentiality disclosures (Greenwald, G. 2014.), is a key example of just how much information is being collected on a daily basis. This specific event raised discussions of the nature, legality, and evolution of data collection and analysis processes.

Research Questions:

1. Why is the government monitoring Internet and social media searches?
2. In what ways is the government How does the government pool its data for analysis?

**Methods**

Participants

The study involved the first seventy undergraduate students at Salisbury University regardless of their class status, whether it be freshmen, sophomore, junior, or senior. Of those seventy, the most common majors of the students who participated were Communications, Education, and Psychology. All participants were at least 18 years of age. Additionally, the participants came from a variety of different lifestyles prior to attending Salisbury Univerity.

Procedures

  The participants completed a 9-question survey (See Appendix A) strictly online and distributed through Survey Monkey. They could take as long as they wanted to develop their answers before submitting the survey. Multiple-choice questions were asked about age requirements, class status, average daily technological use, and knowledge of the government monitoring these platforms. Five short answer questions related to the participant’s three most used applications, government surveillance through various platforms, and opinion-based questions about their possible violation of privacy. The research professor distributed the survey through the “all student” Salisbury email to all current undergraduate students, along with the consent and disclosure forms. The survey was initially distributed on April 1, 2019 and was open for approximately two weeks. The survey was closed on April 16 and the results submitted were finished after the first seventy students submitted their answers.

 Next, it was the researcher’s job to analyze that data into numbers that were concise and coherent for future research.

Measurement

 The researchers chose a mixture of qualitative and quantitative questions to fully examine the scope of which students at Salisbury University understand the extent of government monitoring. Similar data was grouped into categories that were further analyzed in their meaning and significance. The goal in this was to look for trends in these results to see if there were any common ideas among the sample students as to why the government would be monitoring their personal data. The survey focused on the humanistic paradigm, which focuses more on behavior, and critical paradigms, which tend to favor challenging the assumptions of the variable being researched. The researchers calculated the mean and the range of the quantitative data after the survey was completed.

**Results**

Question 1 of survey asked students to report on their gender. offered them the choices of male, female, non-binary, or other. only had students answer male (41.43%) or female (58.57%). No one who took the survey identified as non-binary or other.

 Question 2 of survey asked students to identify their major. The top three most common responses were communication arts at 27%, education at 20% and psychology at 19%. The remaining 44% was divided between computer science, nursing, management, and biology/chemistry.

 The third question of the survey asked students to estimate approximately how long they spent on their phone, tablet, or computer. Approximately 5.71% said they were on their devices less than two hours each day. Students who were on their devices from two to four hours a day made up 27.14% of the results. The largest group was 32.86% of the respondents using their devices between 4-6 hours each day. From there it began to decrease again; 32.43% of respondents reported being on their devices from 6-8 hours a day and an additional 10% reported they were on their phones from 8-10 hours in one day. Finally only 2.86% reported being on an electronic device for more than ten hours in one day.

 Students were asked to rank their most commonly used applications for the fourth question. Participants were provided examples such as Snapchat, Music, and Weather. Many of our respondents reported using music apps such as Spotify (2.3%) or Samsung music (1.7%), which was not helpful for data. However the students that did provide social media apps supplied that their most used social media apps were Snapchat, Instagram, and Twitter.

 The fifth question asked students if they thought the government was monitoring their computer use. The majority of students (74.29%) replied yes, while an additional 10% said no, and the final 15.71% of students were unsure of the government’s role in watching online traffic. Question six went hand in hand with the previous question, asking students to explain their previous answer. One of the students who answered ‘yes’ to the previous question stated that “If I look up something on the computer / phone or talk about something near either of those devices, and ad for that exact thing shows up almost immediately.” Another response from a student who selected ‘yes’ said “I think they’re monitoring [phones] because they have the power to do so and I feel as though they keep things from the public so they need to monitor to make sure nothing horrific is being planned.” On the other hand, there were many responses saying things similar to “I don’t really care enough to have an answer.” Since there is no way of determining which option that student voted for, we have no way of linking the two.

 Question seven asked students if they believed the government was watching its citizens through their laptop cameras. These results were all within 5% of what the students answered for the previous question, so they generally felt the same toward this question as well. One of the students who said ‘no’ also said “not necessarily, unless there is a present and clear reason such as national security.” On the other hand, a different student replied “Yes, I believe that the government is tracking through citizens’ laptop cameras as it is a method of easy monitoring if a person doesn’t know what to look for. For me, there have been several instances where my laptop camera has turned on without me turning it on while in use. Attempts to cover or turn off the camera have been met with reduced computer function until unblocked.”

 Question eight asked students if they believed the government is monitoring you through your phones with call, text, and location data. Students who replied yes, the government is listening to us made up the majority of the population, falling at 71.42%. One of the responses in this category explained “because in order to ‘protect’ the American public they monitor our texts, calls, and locations to stop potential acts of terrorism or violence to us but in order to do that they have to monitor and ‘field’ our calls, texts, and location data. The remaining 14.23% said no, and the same number declared they were unsure. One of the responses for no said that “that information is used mainly be companies that can give the information to the government but the government itself doesn’t do the monitoring.”

 Our final question asked students if they felt their privacy was being violated by the government. This one was interesting because less than half of the respondents (47.88%) felt that their privacy was compromised, 32.81% said no, their privacy was not an issue, and the remaining 20.31% said that they did not know how to feel about their privacy, or some said that it was not the government per se, but Google or another third party. Some who said no, their privacy was not being violated said that the government is simply doing their job to protect this country whereas some who said yes blamed it on the illuminati, and that their phones and personal lives are meant to be just that: personal.

**Discussion**

The purpose of this study was to dissect the relationship between apps and technology as well as government monitoring within cell phones and laptops. The results gave better insight into technology and if the government is actually monitoring society. Students use their phones and laptops every day, whether it is for school, work, or to communicate with others. It was determined that the most time students spend using their cell phones and laptops is between 4-6 hours a day. It was imperative to record the average time using these types of technology to understand if the government could be monitoring us.

 There were more females than males that took the survey. The amount of females who took this survey was 56.6% compared to the men who took this survey, ranking at 43.4%. The students had a variety of majors, such as Elementary Education, Exercise Science, Psychology, Business Management and more. Out of the seventy undergraduate students surveyed, the most used app was Snapchat The second recorded most used app was Instagram and the third most used app was Twitter. Other apps listed were Facebook, Twitter, Instagram, music, Safari, iMessage and gaming apps. When the students were asked if they think that the government is monitoring their cell phone and computer use, 73.58% responded with yes, 9.43% responded with no and 16.98% responded saying they were unsure. Many students explained their previous responses with saying that when they talk about something or look something up on their phone, ads pop up on their phone for that specific thing. One student responded with saying they know the government is watching us because they are looking for specific people and words. They are tapped into our phones and any other electronics, but the government does not care about personal stuff unless it comes out to be suspicious. Many responses mention the government data-logging our information along with saying that social media platforms and websites sell our data to the government.

 Before, there was a rumor going around that the government was watching people through their laptop cameras. When the students were asked about this, a majority responded with saying they do believe they are being watched through their laptop cameras, as it is easy to hack into them and the government would do so if they have probable suspicions. One student said that there have been many instances where his or her camera has turned on by itself and they will attempt to turn off the camera or cover it. There were also a majority of responses that said no, that it is impossible, it is an invasion of privacy and there is no reason for that to happen.

 When the students were asked if they believe that the government is monitoring them through calls, text and location data, a majority of the students said yes, in an attempt to seek out threats and crime. They believe the government are looking for suspicious people. One response from a student that stood out mentioned that he or she has tested this theory. The student created a phone number and used it to create a Google account. The student later received many calls from telemarketers with that same number. From that, the student believes the government would do the same. One student believes that the government collects data through this type of monitoring to stop crimes. A lot of it deals with crime and safety. There were a couple responses that said no because we are allowing our phones to share our location, and some believe that we are not being tracked through this way but the government has the capacity to do so.

 The final question asked the students if they feel that their privacy is being violated. There was a majority of yes and no responses. Some students feel that their privacy is not being violated as they do not have anything to hide. As for the other students, they believe their privacy is being violated. One student responded saying that everything he or she does is being watched and recorded. There is no privacy anywhere, anymore. There is more information compiled on the average person than anyone would assume. The data supports the claim that the government could be monitoring society.

Limitations

 One of the problems that occurred was the lack of participants and the fact that many students skipped questions, whether they did not care enough to answer or did not know how to answer. This skewed some results because they did not take the survey seriously. If the survey was answered to its fullest potential by a variety of students, results could have been much clearer. Another problem with the way the survey was designed was the fact that we had yes or no questions followed by a separate question asking to explain the above answer. Since the survey was designed that way, there was no way to link an explanation to a yes or no answer. Researchers were forced to rely on context to explain vague yes or no answers.

Future Research

 To further this research, it would be beneficial to expand this study to other universities. By receiving more responses from students, results would be widened and improved, and researchers could find overall trends in whether or not the government is really monitoring society. This study is just the beginning; technology is constantly improving which could lead to other ways of testing this.

**References**

*Dourish, P.* 2004. *"What We Talk about When We Talk about Context." Personal and Ubiquitous Computing 8 (1): 19–30.10.1007/s00779-003-0253-8*

*Fairclough, N.* 1995, London : Longman. Document Type: book; (*AN CDA.FAIRCLOUGH.LONGMAN.AIIE*) [Citation Record], Database: EBSCO Publishing Citations

*Greenwald, G.* 2014. No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York, NY: Metropolitan Books.

*Penny, L. 2014, July 3. Laurie Penny on terror and surveillance: Oh look! There's a new bogeyman on the scene to justify online spying. Retrieved March 13, 2019, from* <https://www.newstatesman.com/politics/2014/06/laurie-penny-oh-look-theres-new-bogeyman-scene-justify-online-spying>

*Soghoian, C., & Pell, S. K.* 2014. Your Secret Stingrays No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy. *Harvard Journal of Law and Technology,* *28* (1), 8-16. doi:10.31228/osf.io/67k8c

**Appendix A**

1. What is your gender? Male Female Non-Binary Choose not to answer

2. What is your major?

3. On a regular basis, how often do you use your phone, tablet, or computer? (Check **ONE answer only)**

❏ Less than 2 hours a day

❏ 2-4 hours a day

❏ 4-6 hours a day

❏ 6-8 hours a day

❏ 8-10 hours a day

❏ More than 10 hours a day

4. Please rank your most often used apps. (Ex. Snapchat, Instagram, Music, Weather)

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. Do you think that the government is monitoring your cell phone or computer use?

 1. Yes

 2. No

 3. Unsure

6. Please explain your previous answer on why you do or do not think that the government is tracking your cell phone or computer.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Do you believe that the government is monitoring citizens you through our laptop cameras? Please explain. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Do you believe that the government is monitoring citizens you through our phones with calls, text, and location data? Please explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. Do you feel that your privacy is being violated by the government? Please explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix B**