

Eastern Kentucky University

Encompass

Honors Theses

Student Scholarship

Fall 2021

Controversial Intelligence Gathering: Deciphering the Actions of the U.S. Intelligence Community to the Public

Rachel E. Lehkamp

Eastern Kentucky University, rachel_lehkamp@mymail.eku.edu

Follow this and additional works at: https://encompass.eku.edu/honors_theses

Recommended Citation

Lehkamp, Rachel E., "Controversial Intelligence Gathering: Deciphering the Actions of the U.S. Intelligence Community to the Public" (2021). *Honors Theses*. 851.

https://encompass.eku.edu/honors_theses/851

This Open Access Thesis is brought to you for free and open access by the Student Scholarship at Encompass. It has been accepted for inclusion in Honors Theses by an authorized administrator of Encompass. For more information, please contact Linda.Sizemore@eku.edu.

Eastern Kentucky University

**Controversial Intelligence Gathering: Deciphering the Actions of the U.S. Intelligence
Community to the Public**

Honors Thesis

Submitted

In Partial Fulfillment

Of the

Requirements of HON 420

Fall 2021

By Rachel Lehkamp

Faculty Mentor

Dr. Brian Simpkins

Department of Safety and Security

**Controversial Intelligence Gathering: Deciphering the Actions of the U.S. Intelligence
Community to the Public**

Rachel Lehkamp

Dr. Brian Simpkins; Department of Safety and Security

Abstract description: Following the devastating attacks of 9/11, the U.S. Intelligence Community, or the IC, has made drastic changes within the United States in the name of national security. A major change the IC implemented was initiating constant electronic surveillance of U.S. citizens. This constant surveillance has instilled a growing divide between members of the public who do support government surveillance and those who do not. To assess this divide, an amateur survey was conducted on the Eastern Kentucky University (EKU) campus that included participants of Homeland Security majors and students of other degree programs at the university. The purpose of this survey was to identify if there exists a difference between those who have had background study on the IC and those who have not. The hypothesized results of this survey estimated that Homeland Security majors are to be more forgiving and defendant of the IC's actions while students of other majors and colleges are less forgiving and more accusatory toward the IC of infracting on their privacy rights. Because this survey was conducted in an amateur manner and held several limitations, the data collected could only be analyzed through which what trends *seem* to occur. Thus, the data from this survey *seems* to support the original hypothesis, concluding that having background knowledge on the IC does *seem* to result in people to be more supportive of its actions in the name of national security.

Keywords and phrases: Eastern Kentucky University, government surveillance, homeland security, honors thesis, Intelligence Community, participant data, survey, undergraduate research.

Table of Contents	Page
List of Figures.....	iv
List of Tables.....	v
Acknowledgments.....	vi
Introduction.....	1-6
<i>Objective</i>	5-6
<i>Significance of Research</i>	6
Literature Review.....	6-14
<i>Government Whistleblowing</i>	8-11
<i>Digital Surveillance Dilemmas</i>	11-12
<i>Privacy-Privacy Tradeoffs</i>	12
<i>Argument for the Creation of a new Intelligence Agency</i>	12-14
Methods.....	14-19
<i>Survey Questions</i>	14-17
<i>Participant Categories</i>	17-18
<i>Limitations</i>	18-19
Results.....	19-32
<i>Failure to Complete Theories</i>	20
<i>Statistical Results</i>	20-29
<i>Qualitative Analysis of Results</i>	30-32
Discussion of Results.....	33-34
Conclusion.....	34-35
Appendix.....	36-37
References.....	38-41

List of Figures	Page
Figure 1.....	22
Figure 2.....	23
Figure 3.....	25
Figure 4.....	26
Figure 5.....	28
Figure 6.....	29

List of Tables	Page
Table 1.....	19
Table 2.....	19
Table 3.....	21
Table 4.....	22
Table 5.....	24
Table 6.....	25
Table 7.....	27
Table 8.....	28

Acknowledgments

First and foremost, I would like to thank several ECU Faculty members who offered me guidance throughout this project, those being Dr. Brian Simpkins, Dr. Michelle Smith, Dr. Erik Liddell, and Dr. David Coleman. Each of these incredible scholars provided me with invaluable advice and helped me through difficult periods during my research. Their motivation and help contributed tremendously to the successful completion of this project. I would like to express a special thanks to Dr. Simpkins for working with me as my mentor on this project, helping me with every aspect of this project, from choosing the topic, gathering extensive research, and adding the final touches to finish off the project. I absolutely could not have completed this work without his help. I also want to give a quick thank you to Dr. Smith in the ECU Statistics Department for assisting in the analysis of my data as well as helping me understand the limitations in my research and learn from my mistakes so that I may conduct more formal research in the future.

Thank you again to all who helped me. I am forever grateful for your assistance.

Introduction

“Big Brother is watching you” is a phrase coined in 1949 by George Orwell in the infamous novel *1984*. This novel, in which a singular man’s anxieties for the future regarding the ceaseless evolution of technology and the continuous expansion of government surveillance over its citizens are brought to life, was written over 70 years ago. *1984* follows the character Winston Smith as he lives and works as a low-ranking member of the ruling Party within the fictional nation of Oceania. In the novel, Winston gradually forms frustrations against the Party, which come to fruition when he subsequently rebels against the Party through a crime known as “thoughtcrime,” or any free thought that does not conform with that of the ruling Party (Orwell, 1949). In the novel, the Party is run in a totalitarian style regime with an omniscient political leader solely known as Big Brother. As a result, Oceania is left in a dystopian form of society in which free thought, sexual intimacy, and any expression of individuality are all prohibited and severely punishable. The Party maintains its omnipotent presence through constant surveillance of all members of society through telescreens, placed in both public and private areas, that can never be turned off. Thus, no matter where Winston goes, Big Brother is always watching him.

In regard to reality and the post-*1984* era today, an alarming question that remains is how is it that a novel written in 1949 about one man’s concerns for the future of American society and the possibility of it falling into a dystopia, parallels many of the current anxieties held by U.S. citizens regarding analogous issues with the recent controversial intelligence-gathering actions of the U.S. Intelligence Community? The

omnipresent surveillance ideologies present within *1984* seem to eerily correlate with modern U.S. surveillance technologies today such as listening devices on personal user electronics, surveillance systems in almost all public areas, and wide are surveillance through unmanned aircraft systems (UASs) (Nagy, 2014). In the current debates held in Germany regarding government surveillance and privacy rights, privacy is the main line of resistance against security practices that could possibly “undermine the capacity to live and move in public space anonymously” (Cavelty & Leese, 2018, p. 57). The fight to protect privacy rights remains the final defense against the ideologies of Orwell’s *1984* becoming reality.

Although the U.S. government is a democracy rather than a totalitarian regime and may not be listening to and watching every single interaction each of its citizens are making, there are still violation of privacy rights anxieties that exist among U.S. citizens (Best et al., 2011). In this sense, “information privacy refers to the desire of individuals to control or have some influence over data about themselves” (Bélanger & Crossler, 2011, p. 1017). For some anti-surveillance supporters within the United States today, these privacy anxieties have grown so deep that they have adopted the quote, “1984 was not supposed to be an instruction manual,” as the rallying outcry of their protests against mass government surveillance and the invasion of the privacy rights of U.S. citizens. Other Americans admit having no anxieties regarding government surveillance as they believe it is essential for the protection of the United States from devastating attacks. Many of these anxieties derive directly from the recent actions of government whistleblowers, causing the controversial surveillance actions of the U.S. Intelligence Community to fall under intense scrutiny.

The rise in government surveillance within the United States predominately stems from the shocking attacks of September 11, 2001. The attacks of this tragic, devastating day confirmed the suspicions of the National Security Agency (NSA) that U.S. enemies utilizing integrated global communication networks already existed inside the United States and could make use of e-mail accounts registered within the United States even when not physically in the country (Hayden, 2014). As a result, the Intelligence Community, or the IC, has made drastic changes within the United States in the name of national security (Burney, 2007). A major change the IC implemented was initiating constant electronic surveillance of U.S. citizens. In this sense, “electronic surveillance generally refers to any activity whereby intelligence or police officials: (a) intercept communications in transit or (b) access stored communications” (Forscey & Eoyang, 2016, p. 1). The issue of electronic government surveillance in the United States continues to entice a major debate regarding its necessity.

One of the most important lessons learned from 9/11 was that the attacks were not the result of lack of information. In investigating the events leading up to the attack, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) concluded that U.S. intelligence had received substantial, quality information regarding al-Qaeda’s intentions to attack the United States, including the possible date of such an attack (Barnea, 2019). The IC failed in this case as it was unable to connect the information to formulate a clear picture of the threat, leading to even the most relevant intelligence information to not be shared with various agencies as a consequence of the lack of cooperation and unnecessary compartmentalization that had existed over many years (Barnea, 2019). As a result of this failure, Congress passed into

law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act on October 26, 2002, which began the engagement of the U.S. government in additional controversial surveillance activities as an attempt to deter and punish terrorist acts both within the United States and around the world (Podesta, 2002). Thus, the U.S. IC insisted that the mass surveillance of U.S. citizens was essential in combatting terrorism:

“After the terrorist attacks of September 11, 2001, the Bush Administration established a secret electronic surveillance program to collect data and search for terrorist communications. Under that program, known internally as Stellar Wind, Administration officials negotiated with telecommunications companies to obtain, on U.S. soil, their foreign-to-domestic traffic and did so without obtaining court warrants” (Eoyang & Ashcroft, 2017, p. 2).

The USA Patriot Act ultimately went far beyond what most Americans and lawmakers imagined the law had authorized (Siemion, 2016). Post 9/11 political initiatives such as the USA Patriot Act and programs such as the Stellar Wind subsequently led to the current infringement of American privacy rights, unlawful surveillance, and many other controversial actions conducted by the U.S. IC today.

For years, the public was unaware of the exhaustive measures in which the IC was taking to constantly have surveillance on U.S. citizens, and, quite frankly, the public did not care so long as the measures being taken were justifiable by ensuring national security and preventing future attacks against the United States. This laissez-faire approach of the public, however, gave the IC free reign access to invade the privacy of any, and all, U.S. citizens. These actions remained incredibly well hidden by the

government until the revelatory actions of government whistleblowers such as Edward Snowden and Chelsea Manning, known formerly as Bradley Manning. The whistleblowing actions of these individuals opened the eyes of the public to the in-depth measures the IC was taking to observe U.S. citizens, mainly in times not relative to national security; however, some Americans see these invasive actions as vital in the protection of homeland security and necessary for keeping the United States free from terrorism. Thus, tensions have risen, and the public has become either suspicious, untrusting, or supportive of the IC's actions regarding mass surveillance in the name of national security.

Objective

As a result of the growing divide between members of the public who do support government surveillance and those who do not, the following research was conducted to assess how the public views the controversial actions of the IC in the past two decades with the objective of identifying if having previous, formal knowledge regarding the IC impacts opinions regarding government surveillance. To do so, a survey was conducted on the Eastern Kentucky University (EKU) campus that included participants of Homeland Security majors and students of other degree programs at the university. The purpose of this survey was to identify if there is a difference between those who have had background study on the IC and those who have not. The intention of surveying these two target groups is to determine if having prior knowledge changes how students view the IC's actions and ethicality. The hypothesized results of this survey were estimated to vary drastically between the two factions. Homeland Security majors were estimated to be more forgiving and defendant of the IC's actions while students of other majors and

colleges will be less forgiving and more accusatory toward the IC of infracting on their privacy rights, thus supporting the claim that the controversial actions of the IC have instilled distrust between the government and members of the public unaware of the true intentions of the IC's actions.

Significance of Research

The public plays a major role in ending the infringement of their personal privacy rights. Therefore, the following research is significant to each citizen within the United States because it presents the opposing viewpoints regarding the IC's controversial and invading actions within the past two decades. Everyone within the United States has had their privacy invaded by the IC in the name of national security; however, can these actions be justified when the citizens of the United States no longer feel they have freedom in the supposed free world? The following analysis questions the ethicality of the IC's actions and assesses how the public is concerned regarding their own privacy rights.

Literature Review

Due to growing public concern of the IC's infringement actions on privacy, the scholarship regarding this topic has grown exponentially over the past decade. Since whistleblowing actions by Snowden, Manning, and others, experts have debated the legality and ethics of U.S. government surveillance (Bamford, 2016). Some argue that the issue of privacy versus national security is rather a matter of public perception than it is about losing fundamental liberties:

“In terms of civil liberties, the collection of Big Data does not really affect people. In terms of personal freedom and privacy, the debate is more sensitive, but still not the scary Orwellian scenario of *1984*” (Galantonu, 2016, p. 62).

Evaluating privacy versus national security is a difficult matter because “it is as ‘individuals’ that we are said to seek privacy, but as ‘citizens’ we demand protection from harm; it is ‘the privacy we desire’ versus ‘the security we need’” (Raab, 2017, p. 85). This provides a dilemma within the debate of government surveillance regarding privacy versus national security. In order for security to be provided, some aspects of privacy must be sacrificed.

Although Americans may not be physically impacted by mass government surveillance, there are still many who are uncomfortable with the government having access to their personal information. In a similar sense, a member of the Royal Institute of Town Planning in Britain is quoted as stating,

“I am old enough to remember, you know, when CCTV started and shadows of all of *1984*, and we can't possibly have this, and there were real civil liberties issues about the idea of spy cameras. Now, I think in this country, to a greater extent than I am aware of anywhere else, they are accepted as simply a fact of life” (Goold et al., 2013, p. 980).

Although this was not stated by an U.S. citizen, it shows how government surveillance has evolved to become a key aspect of almost all developed societies today, and that there are many people who have witnessed the evolution. The rapidness of the evolution of government surveillance is what has caused so many to develop major anxiety issues regarding the issue.

For the most part, U.S. citizens would not even be aware of the IC's controversial intelligence gathering actions if it were not for actions of government whistleblowers. The act of government whistleblowing is defined as "the unauthorized acquisition and disclosure of sensitive and classified information regarding the state or government by employees within government agencies" (Delmas, 2015, p. 78). The American public is split into two major groups of opinions regarding government whistleblowing and government surveillance: those who support these actions, insisting they are essential for protecting the United States, and those who do not support these actions, declaring whistleblowers as traitors and government surveillance as an invasion of their privacy rights.

Government Whistleblowing

Candice Delmas (2015), professor of philosophy and political science at Northeastern University, argues that government employees are morally obligated to maintain their oath to secrecy regarding the confidential information they work with; however, the decision to disclose said information to the public can be justified as it is also their duty to report government abuse or the prospect of benefiting from public deliberation (p. 79). Whistleblowing can be considered both patriotically loyal and disloyal in that government whistleblowers are disloyal to their agencies and the safety of the United States; yet they can be considered loyal to their fellow citizens as they disclose potentially harmful information to the public regarding the unethical actions the government has been taking.

Government whistleblowers take it upon themselves to identify certain aspects related to intelligence collection and analysis as unethical and illegal. They feel it is their

duty to inform and the rights of the U.S. citizens to be informed of the questionable actions of the IC. These acts, seen as treasonous by the government and patriotic by the public, can be categorized as intelligence failures due to the unauthorized release of sensitive and confidential information by federal employees. Allison Stanger (2019), professor of international politics and economics at Middlebury College, explicitly argues the act of whistleblowing is vital to the health and proper functionality of American democracy and necessary in strengthening trust between the public and the government within the United States (p. 6). Stanger (2019) explains government whistleblowers are necessary as their actions help to keep the IC ethical and held accountable. Due to the consistent evolution of current technologies and increasing militarization of government agencies within the United States, the expulsion of governmental misconduct has become increasingly difficult and personally detrimental to the individuals who choose to expose said confidential information (Stanger, 2019). This dangerous environment is incredibly impactful on American freedom as many Americans believe it is reliant on the activities and actions of whistleblowers to keep the government honest.

In 2013, Edward Snowden committed one of the most well-known acts of government whistleblowing against the United States to date. He leaked a large, unknown number of gigabytes containing highly classified information about “top-secret plans to counter Chinese cyberattack capabilities, along with detailed budget justifications touching everything NSA does” (Van Cleave, 2013, p. 3). Thanks to Snowden’s historic act of betrayal, the documents leaked revealed many NSA practices, including how it undertakes surveillance activities, introduces security vulnerabilities into products and services, or compels the private sector to cooperate in these activities (Cate, 2015).

Following Snowden's actions, Hogan J. in the court case *Schrems v DPC* came forward identifying the NSA's actions as

“a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance program” (Mulligan, 2016, p. 201).

The unsupervised program Hogan J. identifies is known as PRISM, which was a mass electronic surveillance program operated by the NSA that had equivalent programs operated by the UK and other countries (Penney, 2016). Snowden's revelations were majorly centered around the unlawful PRISM program. Despite mass media reporting on global-scale state surveillance issues following Snowden's exposure of PRISM and the controversial actions of the NSA, the public's privacy behaviors have hardly changed (Preibusch, 2015). This likely results from Americans feeling distant from the issue because they believe no considerable harm has been done. Media attention also focuses too intently on privacy issues and fails to identify the possible benefits to society that big data provided by government surveillance may yield (Reilly, 2015). Big data systems can be incorporated into the intelligence analysis process for IC organizations allowing for a greater amount of information to be available to properly mitigate possible attacks.

As the public became aware of how much access the NSA, and the government in general, had to the everyday American's personal data, many grew to be wary of these actions and sought out means to reduce the government invading their privacy.

Snowden's release of the NSA document cache reveals the vital need to reevaluate the role of government surveillance systems in an age of neoliberal global capitalism (Price,

2014). There are several avenues of resistance that exist so that the everyday Americans may resist or alter the conditions of government surveillance: “We can vote for privacy-friendly politicians, challenge surveillance in court, adopt encryption or other technologies, and put market pressure on companies not to cooperate with law enforcement” (Calo, 2016, p. 23). Adopting these strategies can help reduce government surveillance on personal devices; however, they cannot altogether eradicate government surveillance as it has grown into one of the top lines of defense for U.S. national security.

Digital Surveillance Dilemmas

In analyzing the necessity of government surveillance, it is common that some issues arise. H. Akin Ünver (2018), associate professor of international relations at Kadir Has University, thoroughly explores such dilemmas and deadlocks regarding digital surveillance, the extent it holds in democracies and autocracies, and how it interacts with the surveillance-industrial complex (SIC) (p. 1). Ünver (2018) primarily argues that the ever-evolving methods and technologies utilized in surveillance is a central reason why efforts to regulate and safeguard surveillance mechanisms fail (p. 1). This is because these mechanisms cannot keep up with the constant evolution of intelligence agencies’ technology, nor the incredibly resourceful citizen-driven circumvention tools (Ünver, 2018). Similarly, the failure of government surveillance transparency with the public stems largely from technological backwardness of safeguard and oversight mechanisms. Ünver’s (2018) research revealed this results in an environment in which the public “devises its own mechanisms to circumvent, mask, or monitor how states manage and process digital intelligence and citizen data” (p. 1). In the face of the growing threat of terrorism, far-right radicalization, and extremist groups, the public currently views

surveillance as not only politically necessary, but also electorally popular. Therefore, public opinion has thus split between pro-surveillance and pro-privacy groups, as previously mentioned.

Privacy-Privacy Tradeoffs

Another opinion regarding government surveillance that exists is the idea of privacy-privacy tradeoffs. David Pozen (2016), Vice Dean for Intellectual Life and Charles Keller Beekman Professor of Law, presents the phenomenon of privacy-privacy tradeoffs. Privacy-privacy tradeoffs occur when people are willing to tradeoff some aspects of privacy to ensure the protection of specific privacy aspects: “Privacy-privacy tradeoffs arise when securing privacy on a certain margin compromises privacy on another margin” (p. 221). In doing so, special attention must be paid to the role they play in NSA surveillance. Pozen (2016) presents that legal and policy debates regarding privacy revolve primarily around conflicts between privacy and other goods as well as the idea that privacy clashes with social values as well as privacy itself (p. 221). Pozen (2016) argues such tradeoffs, however, ultimately intrude in modern society and evolving typology. The issue with privacy-privacy tradeoffs is that not all citizens will agree to the same tradeoffs. What people are willing to tradeoff will differ because certain aspects of privacy will be more important to some than others.

Argument for the Creation of a new Intelligence Agency

Some existing arguments support the idea of creating a new intelligence agency solely focused on government surveillance. Genevieve Lester, De Serio Chair of Strategic Intelligence at the U.S. Army War College, investigates the acceptability of a new agency created solely for the collection and analyzation of domestic

counterterrorism (CT) activities, and how useful it would be to the American public.

Lester (2009) argues that American values, ethics, and idiosyncratic form of democracy add specific cultural and complex layers to the domestic intelligence and homeland security efforts (p. 79). The societal acceptability, in this sense, is assessed within the context of the dynamic, post-9/11 national security movement. Lester's (2009) main focuses with this analysis are as follows:

- Address the question of public sense of need for a new agency devoted solely to the domestic CT efforts.
- Investigate the willingness of the public to trade-off civil liberties for security assessing what the public feels is an appropriate balance between the two.
- Analyze the public perception of CT measures and the potentially invasive forms of surveillance and other information gathering techniques as a trade-off for individual expectations of personal privacy.
- Address the triangular relationship among public trust, credibility, and effectiveness in regard to a potential domestic CT intelligence agency.

In her analysis, Lester (2009) finds that due to the threat of terrorism combined with the sense of effectiveness of the current CT structure, the public perception and acceptability of a domestic CT intelligence agency is highly likely. The main question that remains is how much personal privacy the public would be willing to trade-off in the name of national security.

A possible downside of creating a domestic intelligence agency is such an organization would likely represent a protracted effort to collect and analyze intelligence in the United States, calling for more information to be collected on individuals, bringing

about, once again, the debate of privacy issues in consideration with national security (Libicki & Howell, 2009). The willingness of the public to forego personal privacy and civil liberties was only deemed necessary of the public immediately following the attacks of 9/11; thus, despite the continuous threat of terrorism remaining incredibly significant today, the likelihood of the public to trade-off privacy for security purposes remains highly unlikely. With 9/11 having occurred slightly over two decades ago, citizens today are not as fearful of an imminent terrorist attack as they were immediately following 9/11; therefore, they are less likely to be willing to tradeoff their privacy rights for security purposes.

Methods

Resulting from the existing opinions regarding government surveillance, further research on the topic is warranted to assess if having a formal background study on the Intelligence Community and its actions affects how an individual views government surveillance. To test the aforementioned hypothesis that Homeland Security majors are estimated to be more forgiving and defendant of the IC's actions while students of other majors and colleges are less forgiving and more accusatory toward the IC of infracting on their privacy rights, an amateur survey was conducted on EKU's campus that encouraged participation from any EKU student interested in this topic.

Survey Questions

The survey consisted of 11 questions, several regarding the educational background of the participant and their previous knowledge on the topic at hand, as well other questions assessing the opinions the participant holds in respect to how the IC gathers intelligence on U.S. citizens and whether or not they support the actions of

government whistleblowers. The survey questions presented to the participants were as follows:

1. What is your major(s) here at EKU?
 - a. (Open-Ended)
2. If you are not a Homeland Security major, have you completed or are currently enrolled in any EKU courses related to homeland security, national security, intelligence, and/or global security?
 - a. (Yes or No)
3. If yes to Question #2, please list the homeland security, national security, intelligence, and/or global security courses you have completed and/or are currently enrolled in.
 - a. (Open-Ended)
4. On a scale of 1-5, please rate your agreeance with the following statement:
Government surveillance is a violation of my personal privacy rights.
 - a. (1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree)
5. On a scale of 1-5, please rate your agreeance with the following statement:
Government surveillance is essential for the protection of homeland security and preventing terrorism.
 - a. (1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree)
6. On a scale of 1-5, please rate how affected you feel by government surveillance?

- a. (1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree)
7. Please explain any concerns you have regarding mass surveillance.
- a. (Open-Ended)
8. Please explain whether you believe or do not believe mass surveillance is essential in combatting terrorism within the United States?
- a. (Open-Ended)
9. Please explain whether you do or do not support mass surveillance by the government.
- a. (Open-Ended)
10. Please explain whether you support or do not support the actions of government whistleblowers, such as Edward Snowden and Chelsea (Bradley) Manning, who have exposed government actions related to surveillance?
- a. (Open-Ended)
11. Prior to this survey, what previous knowledge did you have regarding the controversial surveillance and intelligence gathering actions of the government and the Intelligence Community?
- a. (Open-Ended)

Each participant's responses were recorded anonymously within an Excel sheet. From there, the provided responses were thoroughly analyzed through both qualitative and quantitative measures. The questions that required specific rating responses from 1-5 were compiled into statistical tables and figures for straightforward analysis. The open-

ended questions were assessed in qualitative measures, comparing each response amongst the others.

Participant Categories

The survey began with a form dedicated to informing participants on the confidentiality and anonymity aspects of the survey. Following the completion of the informed consent form, participants were asked what is their major/majors; have they taken any courses related to homeland security, national security, intelligence, or global security; and, if so, which classes?

During the analysis of the results, the information provided in these questions was used to separate participants into three categories based on specific criteria relating to having a background in Intelligence Studies. A participant was deemed of having a background in Intelligence if they are currently taking or have completed any of the courses required for the Intelligence Studies Certificate here at ECU. These courses include HLS 401 Intelligence Process, HLS 402 Counterintelligence, HLS 403 Intelligence Analysis, and HLS 430 Terrorism and Violent Extremism.

If the participant is a Homeland Security major and responded as having taken at least one of these courses, then they were considered as having an Intelligence background, and thus, were sorted into a separate category than Homeland Security majors with no Intelligence background. Any participant that responded as having completed all courses required for the Homeland Security major were also considered as having an Intelligence background as HLS 401 is required for the major as well as the Intelligence Studies certificate. The other courses are solely required for the certificate. Any Homeland Security major that responded as having taken several Homeland classes

were not included in the Intelligence Studies background category because their answers were not clear enough to determine if they meet the previously stated Intelligence background requirements. Thus, the three participant categories analyzed during the analysis of the results were as follows: 1.) students that are not Homeland Security majors; 2.) students that are Homeland Security majors, but do not have an Intelligence Studies background; and 3.) students that are Homeland Security majors who do have an Intelligence Studies background.

Limitations

As this research was conducted amateurly, it is important to identify and address the limitations that exist within the results. As previously mentioned, the survey is classified as amateur because there are aspects of the research that were conducted informally, and thus, do not and cannot yield definitive assumptions regarding differences in opinions among ECU students on the topic of controversial intelligence actions. The informal selection of participants via professor assistance, posted flyers, and word-of-mouth announcements held no randomization or variation, thus explaining the drastic differences in Homeland Security participation versus participation from students of other majors. Therefore, the results can only be analyzed through assessing what seems to be a trend or what could possibly be a trend if further, more formal study is conducted in the future that includes both randomization and variation. This could be achieved by selecting participants through statistical randomization.

The provided research was conducted in what is known as a convenience sample, meaning the elements, or participants, were included through manners that are easy or convenient for the investigator. Future research on this topic should yield a

randomization strategy known as a stratified sample. This is when a target population is subdivided into two or more groups based on a single characteristic. In this case, that being whether or not the participant is a Homeland Security major. The elements from each group would then be analyzed in proportion to its groups' representation within the entire population. Although the provided research includes limitations, that does not completely disregard or dismiss the information that was found. Thus, the results of the survey and what trends *seem* to exist among the participants' opinions are as follows.

Results

Overall, there were 153 participants; however, 43 the participants failed to complete the survey, either quitting following the informed consent or after inputting their major. The raw results show that 87 participants reported as being Homeland Security majors, and 59 were students of other majors. The 7 missing figures here were the participants who solely accepted the informed consent but never completed any of the survey questions. Of the 110 remaining participants who filled the survey out to completion, 79 were Homeland Security majors and 31 were students of other majors. Table 1 and Table 2 present the participant participation through the representation of the three different participant categories.

All Participants			Homeland Security Majors		
<i>Homeland Security Major?</i>	<i>Count</i>	<i>Percent</i>	<i>Intelligence</i>	<i>Count</i>	<i>Percent</i>
<i>No</i>	59	40.41	<i>No</i>	40	46.51
<i>Yes</i>	87	59.59	<i>Yes</i>	46	53.49
<i>Missing *</i>	7	0.05	<i>Total</i>	86	100
<i>Total</i>	146	100			

Table 1

Table 2

Failure to Complete Theories

A few theories as to why so many of the Homeland Security majors completed the entire survey while a little under half of the non-Homeland Security major participants decided not to complete the entire survey are as follows. First, many of the Homeland Security students were invited to participate by their professors via email attachments and announcements on Blackboard as well as in person in their classes. This encouraged more Homeland Security responses as the students of other majors were invited to participate via flyers posted around campus and through word-of-mouth invitations. Another possible theory as to why more Homeland Security students participated is because they likely have higher interest levels in this topic, leading them to be more inclined to offer their opinions. Other students likely only participated if they held extreme opinions regarding controversial intelligence gathering techniques. It is also likely that many of the non-Homeland Security students began the survey with the intention to complete it; however, when they were asked if they have taken any courses related to homeland security, national security, intelligence, or global security, they decided not to continue because they figured they would not relate to the topic or felt as though their opinions may not be valid since they do not have a background in Intelligence Studies.

Statistical Results

The first opinionated question within the survey assessed participants' opinions regarding the statement: "Government surveillance is a violation of my personal privacy rights." Table 3 below displays the responses of all participants in the survey, no matter what the major.

“Government surveillance is a violation of my personal privacy rights.”

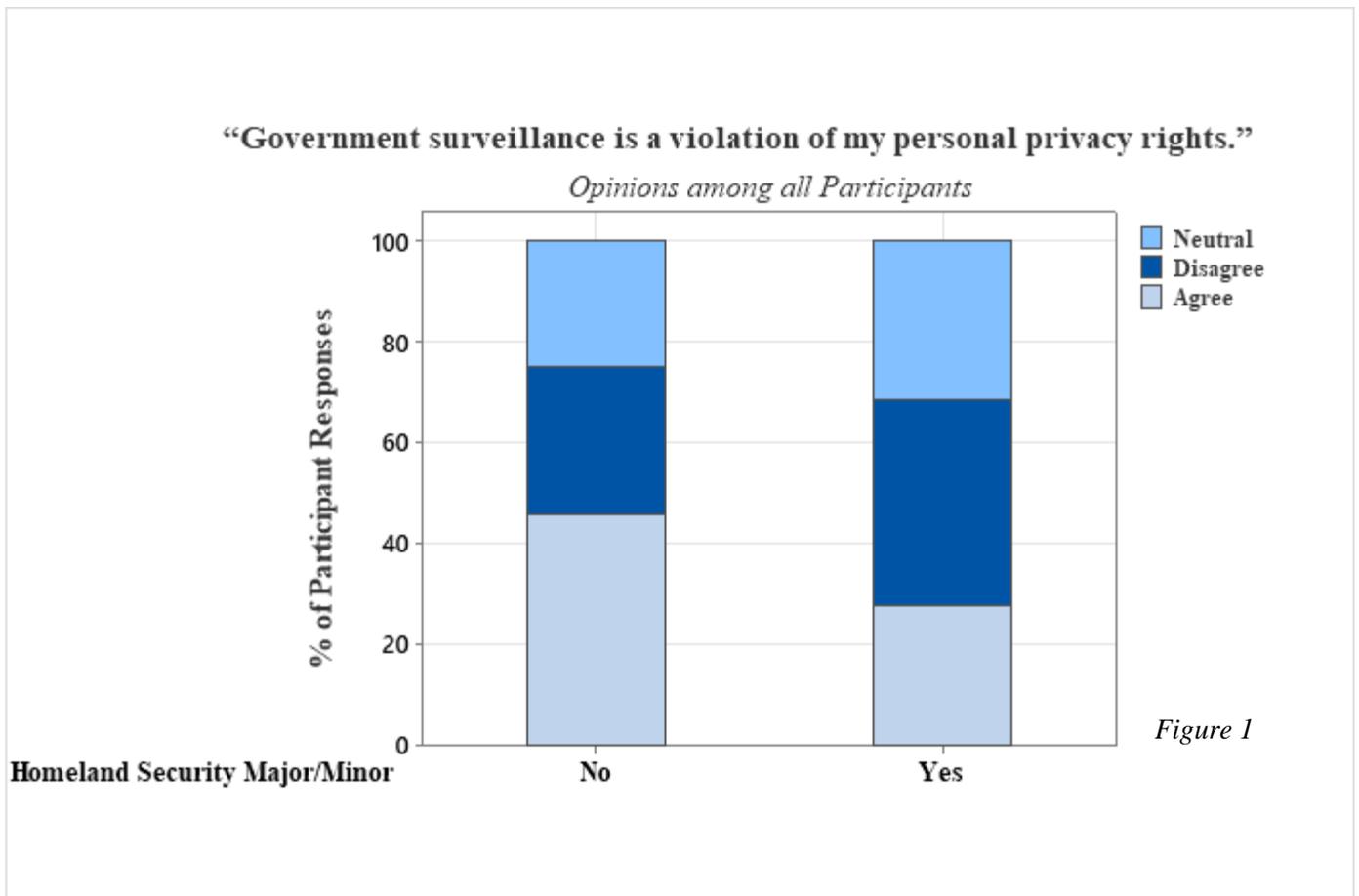
Opinions among all Participants

<i>Homeland Security Major/Minor</i>	<i>Agree</i>	<i>Disagree</i>	<i>Neutral</i>	<i>Missing</i>	<i>All</i>
<i>No</i>	11	7	6	35	24
	45.83	29.17	25.00	*	100.00
<i>Yes</i>	23	34	26	4	83
	27.71	40.96	31.33	*	100.00
<i>Missing</i>	0	0	0	5	*
	*	*	*	*	*
<i>All</i>	34	41	32	*	107
	31.78	38.32	29.91	*	100.00

Table 3

Cell Contents Count % of Row

Table 3 above analyzes the opinions of all participants, comparing Homeland Security major responses against non-Homeland Security major responses. Of the non-Homeland Security participant responses, approximately 46% of the participants agree, 29% disagree, and 25% neither agree nor disagree with the statement. Of the Homeland Security participant responses, approximately 28% of the participants agree, 41% disagree, and 31% neither agree nor disagree with the statement. These results seem to present a noticeable difference between Homeland Security majors and non-Homeland Security majors in which Homeland Security majors seem to be more neutral toward or in support of government surveillance; thus, seeming to support the original thesis statement. Figure 1 below is a visual representation of data within Table 3.



Continuing with the same question, Table 4 below only displays the responses of participants with Homeland Security majors or minors.

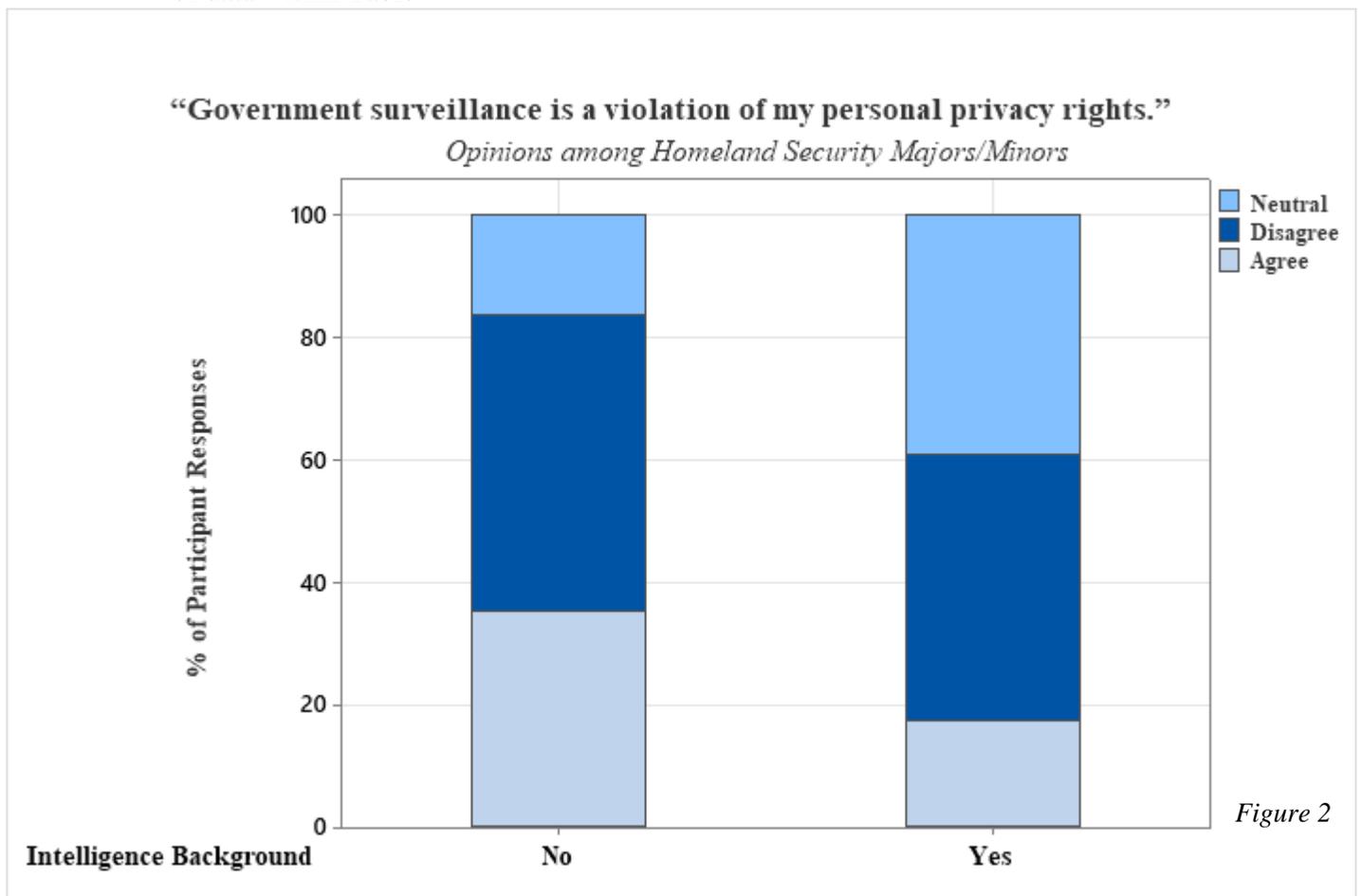
“Government surveillance is a violation of my personal privacy rights.”
Opinions among Homeland Security Majors/Minors

<i>Intelligence Background</i>	<i>Agree</i>	<i>Disagree</i>	<i>Neutral</i>	<i>Missing</i>	<i>All</i>
<i>No</i>	13	18	6	3	37
	35.14	48.65	16.22	*	100.00
<i>Yes</i>	8	20	18	0	46
	17.39	43.48	39.13	*	100.00
<i>All</i>	21	38	24	*	83
	25.30	45.78	28.92	*	100.00

Table 4

Cell Contents Count % of Row

Table 4 more thoroughly analyzes opinions amongst Homeland Security majors, further comparing opinions between students with Intelligence backgrounds against students without. Of the Homeland Security majors who do not have a background in Intelligence Studies, approximately 35% of participants agree, 49% disagree, and 16% neither agree nor disagree with the statement. Of the Homeland Security students who do have a background in Intelligence Studies, 17% of the participants agree, 43% disagree, and 39% neither agree nor disagree with the statement. These results seem to further prove that having a background study in the field of Intelligence allows for a better understanding of why government surveillance is necessary causing these students to be more supportive or neutral regarding the issue. Figure 2 below is a visual representation of data within Table 4.



The next opinionated survey question assessed participants' opinions regarding the statement: "Government surveillance is essential for the protection of homeland security and preventing terrorism." Similar as before, Table 5 below displays the responses of all participants in the survey, no matter what the major.

"Government surveillance is essential for the protection of homeland security and preventing terrorism"

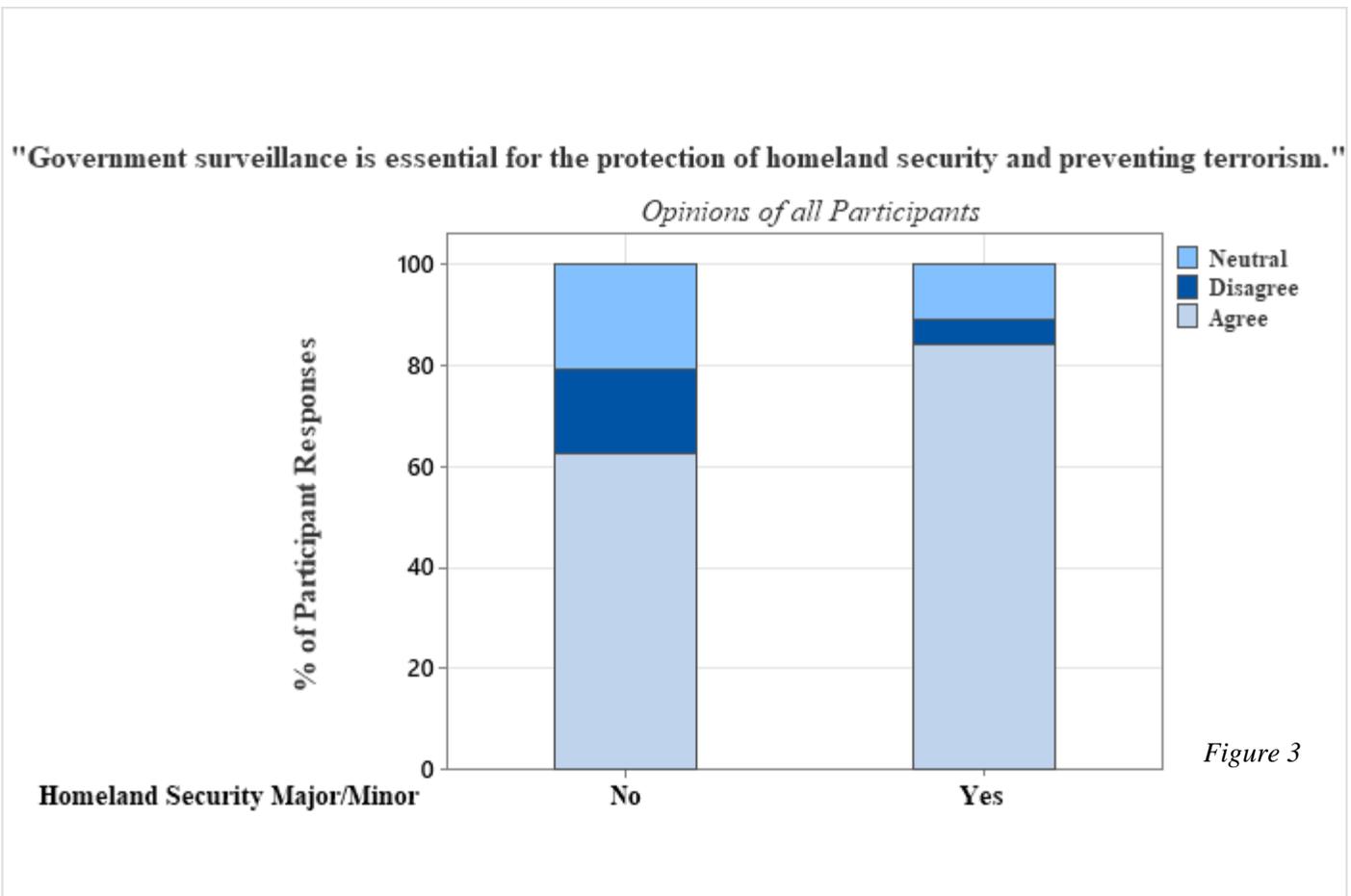
Opinions of all Participants

<i>Homeland Security Major/Minor</i>	<i>Agree</i>	<i>Disagree</i>	<i>Neutral</i>	<i>Missing</i>	<i>All</i>
<i>No</i>	15 62.50	4 16.67	5 20.83	35 *	24 100.00
<i>Yes</i>	70 84.34	4 4.82	9 10.84	4 *	83 100.00
<i>Missing</i>	0 *	0 *	0 *	5 *	* *
<i>All</i>	85 79.44	8 7.48	14 13.08	* *	107 100.00

Table 5

Cell Contents Count % of Row

Of the non-Homeland Security participant responses, approximately 63% of the participants agree, 17% disagree, and 21% neither agree nor disagree with the statement. Of the Homeland Security participant responses, approximately 84% of the participants agree, 5% disagree, and 11% neither agree nor disagree with the statement. These results seem to show that Homeland Security majors are more likely to agree with this statement, most likely as a result of terrorism preventative measures being discussed within the majority of Homeland Security courses. Figure 3 below is a visual representation of data within Table 5.



Continuing with the same question, Table 6 below only displays the responses of participants with Homeland Security majors or minors.

“Government surveillance is essential for the protection of homeland security and preventing terrorism.”

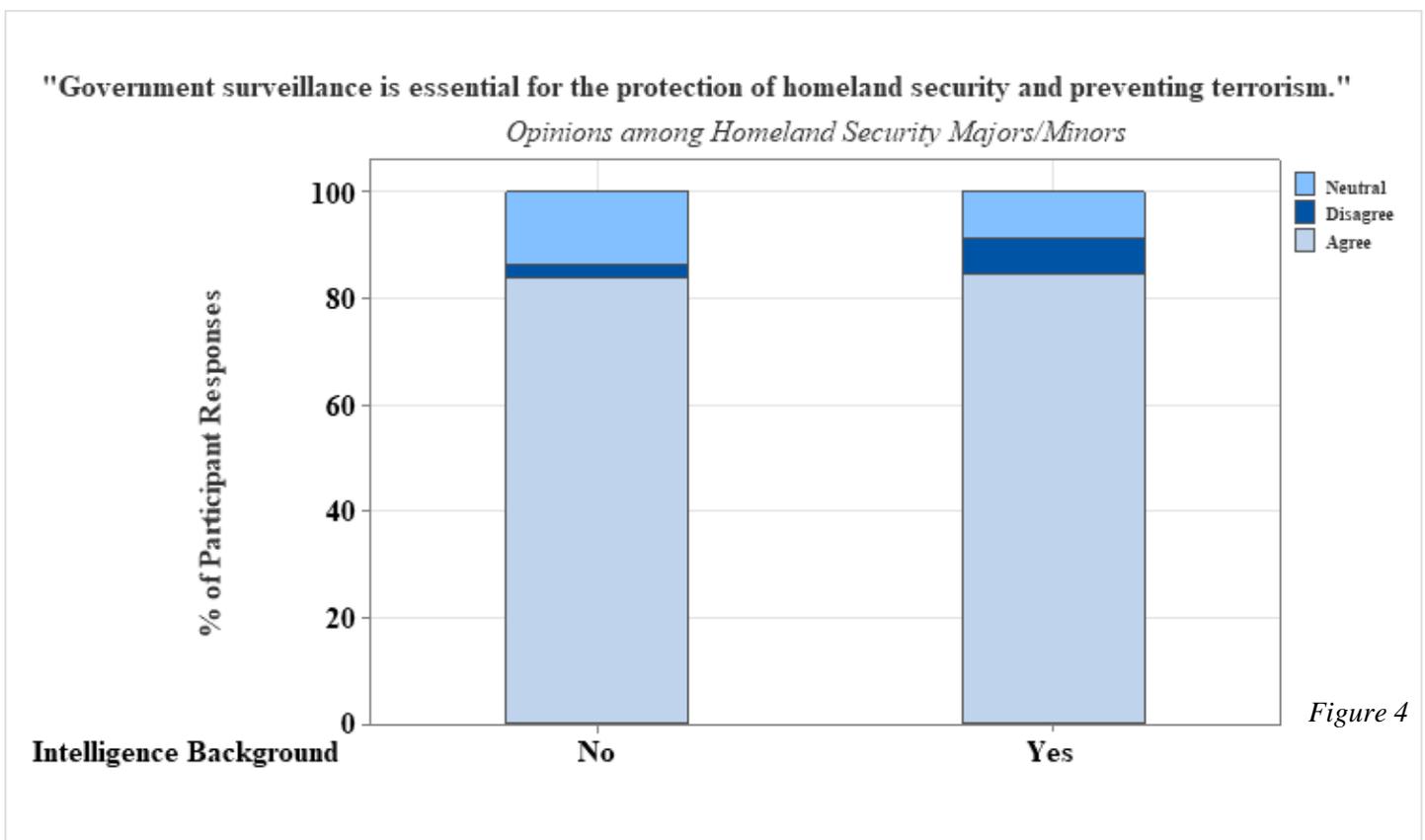
Opinions among Homeland Security Majors/Minors

<i>Intelligence Background</i>	<i>Agree</i>	<i>Disagree</i>	<i>Neutral</i>	<i>Missing</i>	<i>All</i>
<i>No</i>	31	1	5	3	37
	83.78	2.70	13.51	*	100.00
<i>Yes</i>	39	3	4	0	46
	84.78	6.52	8.70	*	100.00
<i>All</i>	70	4	9	*	83
	84.34	4.82	10.84	*	100.00

Table 6

Cell Contents Count % of Row

Of the Homeland Security majors who do not have a background in Intelligence Studies, approximately 84% of participants agree, 3% disagree, and 14% neither agree nor disagree with the statement. Of the Homeland Security students who do have a background in Intelligence Studies, 85% of the participants agree, 7% disagree, and 9% neither agree nor disagree with the statement. These results do not seem to yield any differences in opinion whether the participants had a prior Intelligence background or not. Figure 4 below is a visual representation of data within Table 6.



The final, non-open-ended opinionated question assessed participants' opinions regarding the participants' level of affectedness by government surveillance. Table 7 below displays the responses of all participants in the survey, no matter what the major.

Participants' Level of Affectedness by Government Surveillance

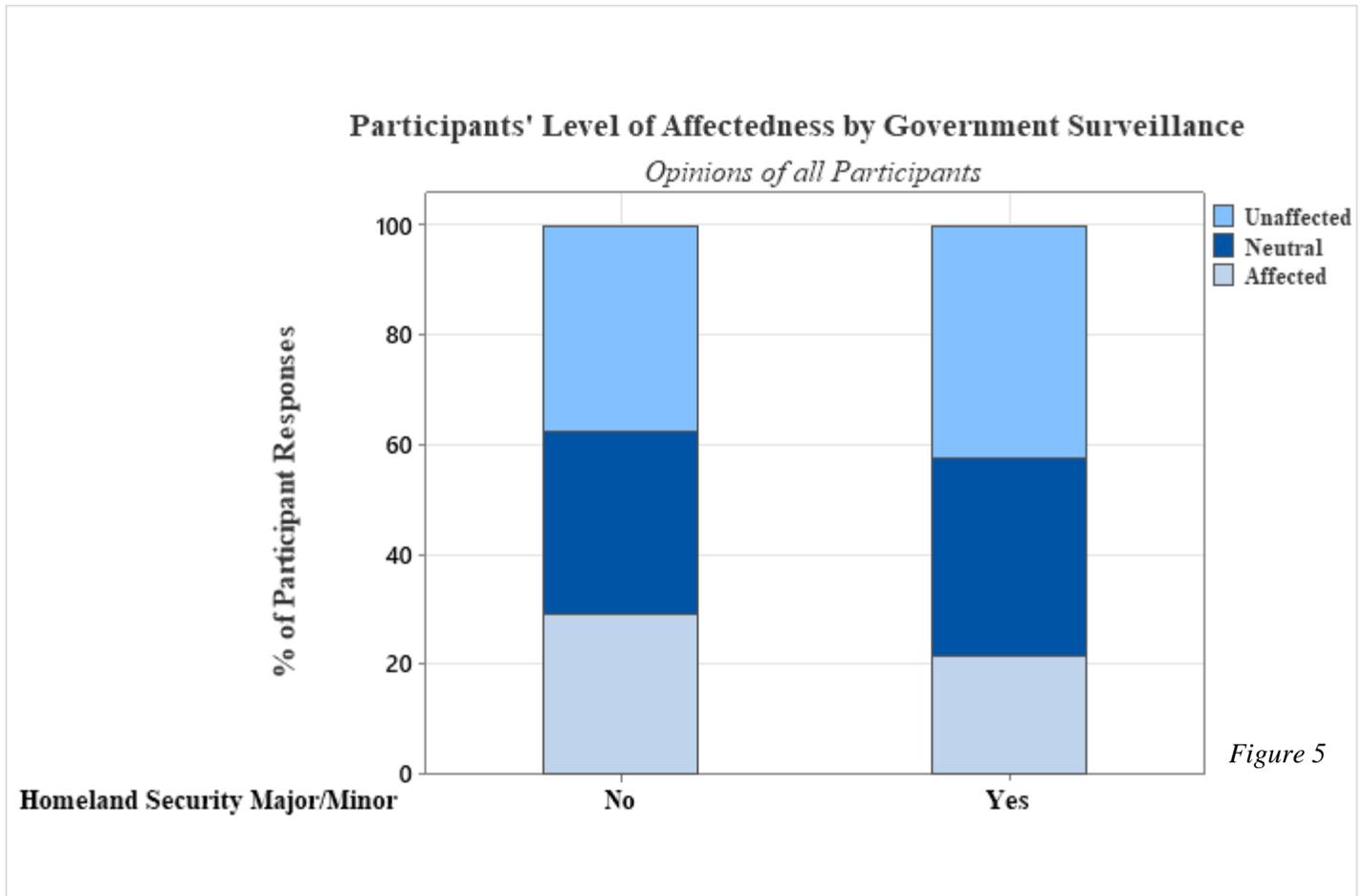
Opinions of all Participants

<i>Homeland Security Major/Minor</i>	<i>Affected</i>	<i>Neutral</i>	<i>Unaffected</i>	<i>Missing</i>	<i>All</i>
<i>No</i>	7	8	9	35	24
	29.17	33.33	37.50	*	100.00
<i>Yes</i>	18	30	35	4	83
	21.69	36.14	42.17	*	100.00
<i>Missing</i>	0	0	0	5	*
	*	*	*	*	*
<i>All</i>	25	38	44	*	107
	23.36	35.51	41.12	*	100.00

Table 7

Cell Contents Count % of Row

Table 7 shows that, of the non-Homeland Security participant responses, approximately 29% of the participants reported that they were affected, 33% felt neutral on the topic, and 38% reported they were unaffected by government surveillance. Of the Homeland Security participant responses, approximately 22% of the participants reported that they were affected, 36% felt neutral on the topic, and 42% reported they were unaffected by government surveillance. These results seem to yield very little differences between the two groups, with the majority of both as reporting feeling unaffected by government surveillance. Figure 5 below is a visual representation of data within Table 7.



Continuing with the same question, Table 8 below only displays the responses of participants with Homeland Security majors or minors.

Participants' Level of Affectedness by Government Surveillance

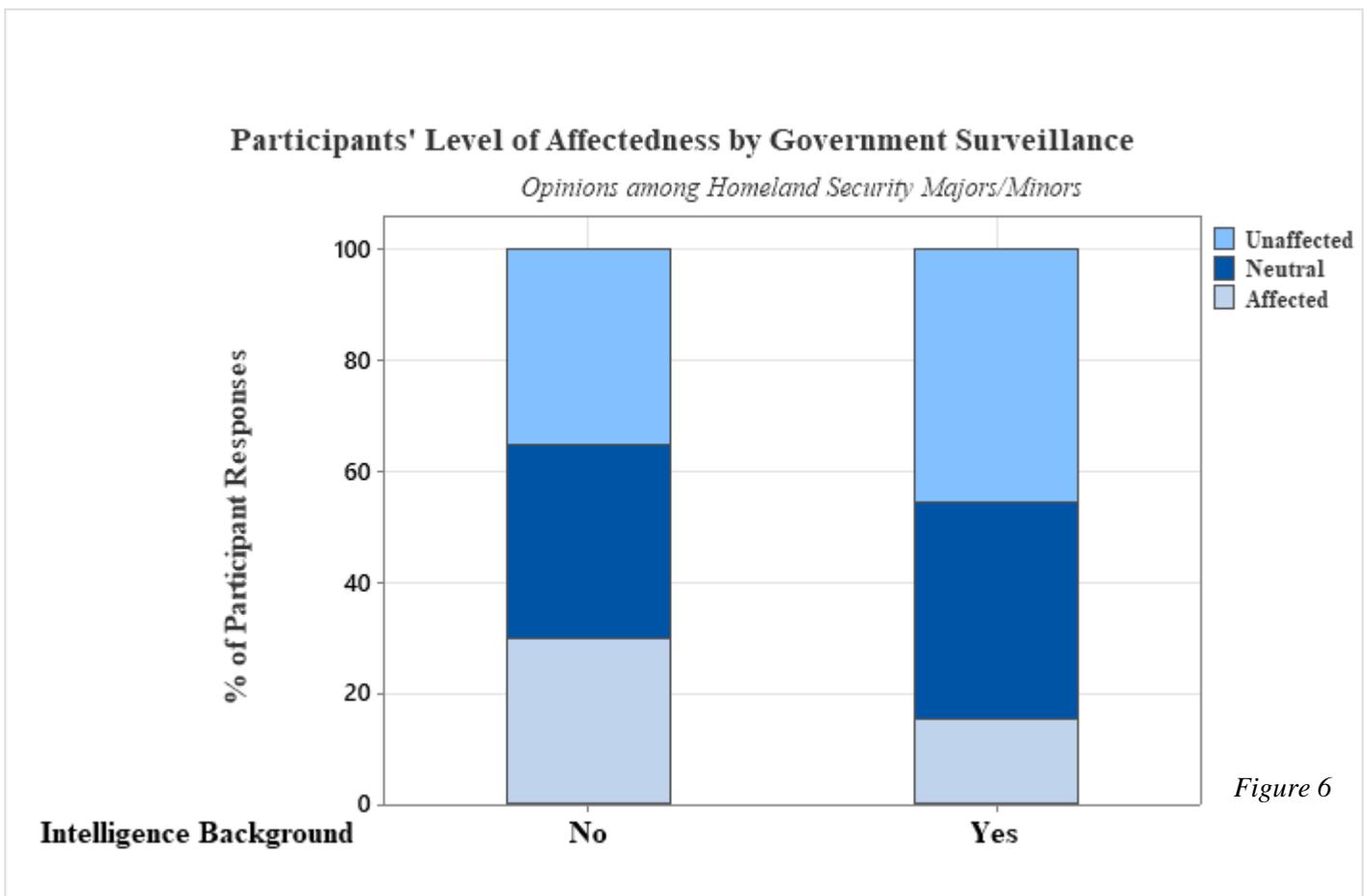
Opinions among Homeland Security Majors/Minors

<i>Intelligence Background</i>	<i>Affected</i>	<i>Neutral</i>	<i>Unaffected</i>	<i>Missing</i>	<i>All</i>
<i>No</i>	11	13	13	3	37
	29.73	35.14	35.14	*	100.00
<i>Yes</i>	7	18	21	0	46
	15.22	39.13	45.65	*	100.00
<i>All</i>	18	31	34	*	83
	21.69	37.35	40.96	*	100.00

Cell Contents Count % of Row

Table 8

Table 8 shows that, of the Homeland Security majors who do not have a background in Intelligence Studies, approximately 30% of the participants reported that they were affected, 35% felt neutral on the topic, and 35% reported they were unaffected by government surveillance. Of the Homeland Security participant responses who do have a background in Intelligence Studies, approximately 15% of the participants reported that they were affected, 39% felt neutral on the topic, and 46% reported they were unaffected by government surveillance. These results seem to show some slight differences in Homeland Security levels of affectedness, with students with Intelligence backgrounds being more likely to report feeling unaffected by government surveillance. Figure 6 below is a visual representation of data within Table 8.



Qualitative Analysis of Results

The open-ended questions of the survey yielded a wide variety of responses from the participants. Each question asked the participants to explain how they feel regarding the topic at hand. The most astounding participant quotes from each question are as follows:

1. *“Please explain any concerns you have regarding mass surveillance.”*

- “I feel like it is very "Big Brother", and someone is watching my every movement”
- “I don’t have any concerns regarding government surveillance, I believe government surveillance is necessary to prevent large scale terror attacks.”
- “I think that it can be degrading toward minority groups prevalent in America and that the surveillance is not done equally”
- “The U.S. government has access to literally everything you've ever done online, talked about over text, email, or the phone, etc. They have every nude anyone has ever sent, every secret someone has ever told to a friend over the phone, every phone message left by someone's doctor's office. There is nowhere near enough oversight, way too much invasion of privacy, and too much risk of all of that information falling into the wrong hands (and honestly, in the government's possession it already has). It is a violation of every citizen’s constitutional right to privacy.”

2. *“Please explain whether you believe or do not believe mass surveillance is essential in combatting terrorism within the United States.”*

- “Surveillance on everyone isn't essential when facing terrorism. Bad actors need to be identified and targeted alone. Targeting everyone will lead to more resistance and possibly even more terrorism.”
- “I believe that it can certainly be an easy option to help combat terrorism, [but] I do not believe that it is the only reason they are doing it.”
- “I believe it is essential. Sometimes you have to do what is perceived as bad to keep a 250+ year old country running.”
- “Although some security is indubitably required, mass surveillance crosses the line between keeping a country safe and oppression.”

3. *“Please explain whether you do or do not support mass surveillance by the government.”*

- “I do support it, as I have nothing to hide from the government. The government is not worried about what the average citizen is doing.”
- “I don't want the government spying on me. I personally feel like it is an invasion of my privacy. If I want someone to know my business, then they will be informed about whatever it is that I want them to know.”
- “I absolutely do not support mass surveillance by the U.S. government. You can't say ‘if you don't have anything to hide, you shouldn't be worried’ because hiding a criminal act and needing privacy are not the same. I wouldn't and don't hide the fact that I have medical conditions or that I am bisexual, but the government does not have any business knowing the nitty gritty of my healthcare or relationships.”

- “I do support mass surveillance in public places, where a right to privacy is not reasonably expected. However, I believe a search warrant or something of the likes should be required for in-home surveillance.”

4. *“Please explain whether you support or do not support the actions of government whistleblowers, such as Edward Snowden and Chelsea Manning, who have exposed government actions related to surveillance.”*

- “No. I do not support them. Keep your mouth close.”
- “I absolutely agree with what Edward Snowden did. Exposing the abuse of powers such as tapping into any given person at any time is horrible, and people were doing this for their own personal enjoyment. Also, look at what happened, with him exposing the government he is now laying low in a foreign country in fear of his life.”
- “I am unsure of who these people are and have not heard much of anything about what they have done. However, anyone purposefully trying to destroy and show how the government catches reformists negatively effects my safety, so I disagree with them.”
- “I do not support whistleblowers because they are leaking information that was made secret for a reason, and not only is information let out but so are methods and sources which can be a devastating loss for the Intelligence Community. Whistle blowers are traitors to the United States.”
- “I absolutely support their actions. The people deserve to know that they are being spied on and that their rights are being violated, and I have nothing but respect for Snowden and Manning.”

Discussion of Results

Overall, the results of the survey generally seem to support the original hypothesis statement that Homeland Security majors are more forgiving and defendant of the IC's actions while students of other majors and colleges are less forgiving and more accusatory toward the IC of infracting on their privacy rights. The greatest disparity amongst opinions seems to be between Homeland Security majors with and without Intelligence backgrounds on the topic of whether or not government surveillance is a violation of the participants' privacy rights, therefore seeming to provide the most support for my hypothesis.

The responses to the open-ended questions yielded a wide variety of opinions regarding the topics discussed in each of the questions. Some of the participants held strong, aggressive opinions, while others were unaware of some of the issues addressed. When asked about whether they do or do not support mass surveillance by the government, many participants responded that they do support mass surveillance for suspicious individuals, but they do not support mass surveillance of innocent, law-abiding citizens. For example, one participant stated,

“I only support surveillance for anti-terroristic reasons. I don't think the everyday individual needs to be watched.”

The issue with this opinion is what constitutes someone as being suspicious? Is it their race, their nationality, their criminal history, their search history, or what? In the same sense, what constitutes someone as an “everyday individual?” This can become a major issue for the government if the IC does not fairly and ethically assess suspicious persons:

“ . . . in a truly open and transparent society where everybody is accountable for their deeds, that does not make any of us necessarily a target of the abuse of power. We all give the same kind of information and receive the same kind of treatment” (Nagy, 2014, 136).

In order for government surveillance to be considered fair, all individuals must be subjugated to the same invasive surveillance. Just because someone seems to be innocent online does not mean they will not commit crimes as well. Thus, mass surveillance is greater than solely searching for suspicious individuals already on the IC’s radar. The purpose of mass surveillance is to identify any suspicious activity conducted by any individual.

Conclusion

After thorough analysis of the results of the survey, it seems the responses do yield support for the original hypothesis that Homeland Security students are more forgiving and supportive of the IC’s actions than students of other majors. Despite the limitations present when conducting the survey, the information that was provided still offered varying and important opinions. As technology continues to evolve alongside society’s reliance on the Internet, the topic of controversial intelligence gathering will only grow to become more prevalent. Therefore, this continuous technological and societal evolution warrants further, formal research on the public’s opinion of the IC’s actions. While the public does not need to know every aspect of the IC’s surveillance techniques, it is important that it remains aware of the basic operations of the IC’s actions. The IC must continuously be checked and balanced to ensure the government complies with the constitutional rights of U.S. citizens. Otherwise, George Orwell was

right, and the omnipresent “Big Brother” presence lingers in the very near future of the United States.

Appendix

Survey Questions

1. What is your major(s) here at EKU?
 - a. (Open-Ended)
2. If you are not a Homeland Security major, have you completed or are currently enrolled in any EKU courses related to homeland security, national security, intelligence, and/or global security?
 - a. (Yes or No)
3. If yes to Question #2, please list the homeland security, national security, intelligence, and/or global security courses you have completed and/or are currently enrolled in.
 - a. (Open-Ended)
4. On a scale of 1-5, please rate your agreeance with the following statement:
Government surveillance is a violation of my personal privacy rights.
 - a. (1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree)
5. On a scale of 1-5, please rate your agreeance with the following statement:
Government surveillance is essential for the protection of homeland security and preventing terrorism.
 - a. (1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree)
6. On a scale of 1-5, please rate how affected you feel by government surveillance?

- a. (1=Strongly Disagree; 2=Disagree; 3=Neutral; 4=Agree; 5=Strongly Agree)
7. Please explain any concerns you have regarding mass surveillance.
 - a. (Open-Ended)
 8. Please explain whether you believe or do not believe mass surveillance is essential in combatting terrorism within the United States?
 - a. (Open-Ended)
 9. Please explain whether you do or do not support mass surveillance by the government.
 - a. (Open-Ended)
 10. Please explain whether you support or do not support the actions of government whistleblowers, such as Edward Snowden and Chelsea (Bradley) Manning, who have exposed government actions related to surveillance?
 - a. (Open-Ended)
 11. Prior to this survey, what previous knowledge did you have regarding the controversial surveillance and intelligence gathering actions of the government and the Intelligence Community?
 - a. (Open-Ended)

References

- Bamford, J. (2016). Every Move You Make. *Foreign Policy*, 220, 56–63.
<https://www.jstor.org/stable/44842760>.
- Barnea, A. (2019). Big Data and Counterintelligence in Western Countries. *International Journal of Intelligence and Counterintelligence*, 32(3), 433-447. DOI: 10.1080/08850607.2019.1605804.
- Bélangier, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), 1017–1041. <https://doi.org/10.2307/41409971>.
- Best, S., Krueger, B., & Pearson-Merkowitz, S. (2012). Al Qaeda Versus Big Brother: Anxiety About Government Monitoring and Support for Domestic Counterterrorism Policies. *Political Behavior*, 34(4), 607-625.
<http://www.jstor.org.libproxy.eku.edu/stable/23359650>.
- Burney, B. (2007). The Patriot Act. *GPSolo*, 24(5), 26–30.
<http://www.jstor.org/stable/23673431>.
- Calo, R. (2016). Can Americans Resist Surveillance? *The University of Chicago Law Review*, 83(1), 23-43. <http://www.jstor.org.libproxy.eku.edu/stable/43741590>.
- Cate, F. H., & Ganguly, S. (2015). Edward Snowden and the NSA: Law, Policy, and Politics. In D. P. Fidler (Ed.), *The Snowden Reader* (pp. 26–44). Indiana University Press. <http://www.jstor.org/stable/j.ctt16gh840.9>.
- Cavelty, M. D., & Leese, M. (2018). Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity. *European Review of International Studies*, 5(3), 49–69. <https://www.jstor.org/stable/26593815>.

- Delmas, C. (2015). The Ethics of Government Whistleblowing. *Social Theory and Practice*, 41(1), 77-105. <http://www.jstor.org.libproxy.eku.edu/stable/24332319>.
- Eoyang, M., & Ashcroft, G. (2017). (Rep.). *Why Electronic Surveillance Reform is Necessary*. Third Way. <http://www.jstor.org.libproxy.eku.edu/stable/resrep02523>.
- Forscey, D., & Eoyang, M. (2016). (Rep.). *Surveillance and Encryption*. Third Way. <http://www.jstor.org.libproxy.eku.edu/stable/resrep02537>.
- Galantonu, D. (2016). The Big Brother Fear: Four Perspectives on Surveillance. *American Intelligence Journal*, 33(1), 59-64. <https://www-jstor-org.libproxy.eku.edu/stable/26202166>.
- Goold, B., Loader, I., & Thumala, A. (2013). The Banality of Security: The Curious Case of Surveillance Cameras. *The British Journal of Criminology*, 53(6), 977-996. <http://www.jstor.org.libproxy.eku.edu/stable/23639949>.
- Hayden, M. V. (2014). Beyond Snowden: An NSA Reality Check. *World Affairs*, 176(5), 13-23. https://www-jstor-org.libproxy.eku.edu/stable/pdf/43555047.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A7bc93d0fc1f6812d3883a3b6163fead5.
- Lester, G. (2009). Societal Acceptability of Domestic Intelligence. In B. A. Jackson. (Ed.), *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency* (pp. 79-104). RAND Corporation. <http://www.jstor.org.libproxy.eku.edu/stable/10.7249/mg804dhs.11>.

- Libicki, M. C., & Howell, D. R. (2009). Privacy and Civil Liberties Protections in a New Domestic Intelligence Agency. In B. A. Jackson (Ed.), *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency* (pp. 149–178). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg804dhs.14>.
- Mulligan, A. (2016). Constitutional Aspects of International Data Transfer and Mass Surveillance. *Irish Jurist*, 55, new series, 199-208. <http://www.jstor.org.libproxy.eku.edu/stable/44027072>.
- Nagy, B. (2014). Why They Can Watch You: Assessing the Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement. *Berkeley Technology Law Journal*, 29(1), 135-174. <http://www.jstor.org.libproxy.eku.edu/stable/24119939>.
- Orwell, G. (1949). *1984*. Secker & Warburg.
- Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal*, 31(1), 117-182. <http://www.jstor.org.libproxy.eku.edu/stable/43917620>.
- Podesta, J. (2002). USA Patriot Act: The Good, the Bad, and the Sunset. *Human Rights*, 29(1), 3–7. <http://www.jstor.org/stable/27880293>.
- Pozen, D. (2016). Privacy-Privacy Tradeoffs. *The University of Chicago Law Review*, 83(1), 221-247. <http://www.jstor.org.libproxy.eku.edu/stable/43741598>.
- Preibusch, S. (2015). Privacy Behaviors After Snowden. *Communications of the ACM*, 58(5), 48-55. <https://doi-org.libproxy.eku.edu/10.1145/2663341>.

- Price, D. H. (2014). The New Surveillance Normal NSA and Corporate Surveillance in the Age of Global Capitalism. *Monthly Review*, 66(3), 43-53.
<https://monthlyreview.org/2014/07/01/the-new-surveillance-normal/>.
- Raab, C. D. (2017). Security, Privacy and Oversight. In A. W. Neal (Ed.), *Security in a Small Nation: Scotland, Democracy, Politics* (1st ed., Vol. 4, pp. 77–102). Open Book Publishers. <http://www.jstor.org/stable/j.ctt1sq5v42.8>.
- Reilly, B. C. (2015). Doing More with More: The Efficacy of Big Data in the Intelligence Community. *American Intelligence Journal*, 32(1), 18–24.
<http://www.jstor.org/stable/26202099>.
- Siemion, R. (2016). Protecting Privacy in the Digital Age: Beyond Reforming Bulk Telephone Records Collection. *Human Rights*, 41(4), 17–20.
<http://www.jstor.org/stable/26423457>.
- Stanger, A. (2019). *Whistleblowers: Honesty in America from Washington to Trump*. Yale University Press.
- Ünver, H. (2018). (Rep.). *Politics of Digital Surveillance, National Security and Privacy*. Centre for Economics and Foreign Policy Studies.
<http://www.jstor.org/stable/resrep17009>.
- Van Cleave, M. (2013). (Rep.). *Myth, Paradox & the Obligations of Leadership: Edward Snowden, Bradley Manning and the Next Leak*. Center for Security Policy.
<http://www.jstor.org.libproxy.eku.edu/stable/resrep05061>.