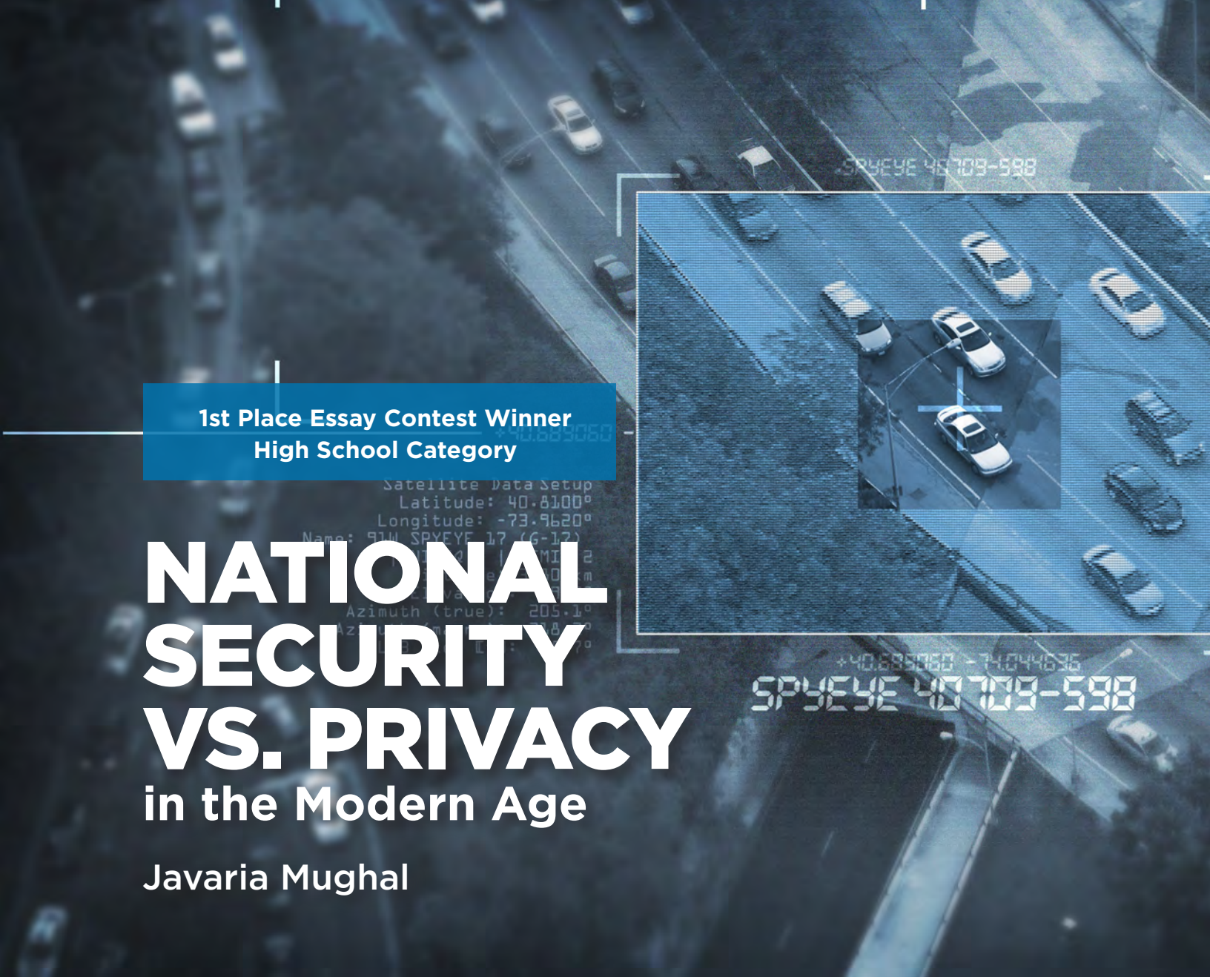

1st Place Essay Contest Winner
High School Category

NATIONAL SECURITY VS. PRIVACY
in the Modern Age

Javaria Mughal

Government surveillance has justifiably developed a negative connotation due to governments' mass accumulation of the personal and communications data of millions of citizens, misleading or overblown claims about the effectiveness of these bulk surveillance programs in preventing terrorist attacks (Bergen, Sterman, Schneider, and Cahall, 2014), and the dubious legal footing of these programs (Associated Press, 2015, May 7; Condon, 2013, June 12). Such problems demonstrate a need to reevaluate the scope of intelligence operations, and the regulations that govern them. However, surveillance remains a necessary component in securing a nation and protecting its constituent citizens.

Today, terrorism poses a legitimate threat to Western countries, as illustrated by the events of 9/11, threats from extremist groups such

as ISIS, and attempted plots on Western countries (Bergen, Sterman, Schneider, and Cahall, 2014). The attacks on 9/11 and the conflicts created by extremist groups in the Middle East demonstrate these terrorist organizations' significant capacities for destruction. To prevent potentially catastrophic attacks on Western countries, governments must use preemptive measures to identify and neutralize possible strikes before they occur. Without monitoring highly suspected persons' communications and activities, government security programs are less able to assess the severity of threats, as their only intelligence sources would be intermittent tips. US intelligence claims to have already stopped dozens of attacks through preemptive investigation and response, yet some analysts believe that these numbers are exaggerated (Bergen, Sterman, Schneider, and Cahall, 2014).

Today, terrorism poses a legitimate threat to Western countries, as illustrated by the events of 9/11 and threats from extremist groups such as ISIS...

Government surveillance can be useful in many domains other than terrorism. Cases involving unwarranted police violence, assault, theft, and murder can be aided through CCTV cameras. In the *State of Florida vs. George Zimmerman* case, eyewitness accounts of the conflict between Zimmerman and Trayvon Martin all differed. Consequently, prosecutors found it difficult to establish a comprehensive picture of the night's events. The presence of CCTV cameras or other visual surveillance equipment could have more clearly established the facts and better enabled the successful prosecution of George Zimmerman, or corroborated his innocence as ruled by the court (Bilton, 2013, July 16). Too often do the facts surrounding injustices come down to the word of those with unreliable knowledge, or reason to lie, and too often do we fail to bring justice, or know if justice has been brought, to those actually guilty or innocent.

To prevent potentially catastrophic attacks on Western countries, governments must use preemptive measures to identify and neutralize possible strikes before they occur.

Having established the usefulness of surveillance, the next step becomes determining the extent to which surveillance is appropriate. In 2013, Edward Snowden leaked evidence of the US government's bulk surveillance programs, including the PRISM program for collecting Internet communications of the bulk telephony metadata extraction justified under Section 215 of the US Patriot Act (Granick and Sprigman, 2013, June 27). Since this release, US government officials have consistently stressed the need for these programs. President Obama defended them as integral to the protection of American citizens (Baker, 2013, June 17). NSA Director

Gen. Keith Alexander stated before Congress that "the information gathered from these programs provided the US government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world" (United States Congress, 2013, June 18). However, a report from the New American Foundation casts doubt on these claims.

How large a role does bulk surveillance play in counter-terrorism efforts?

By analyzing 225 cases involving individuals charged with some terrorism crime, the authors of the report *Does NSA's Bulk Surveillance Programs Stop Terrorists?* determined that NSA surveillance only initiated 7.5% of investigations, of which 1.8% involved bulk telephony metadata under Section 215 of the USA Patriot Act, 4.4% involved surveillance under Section 702 of the FISA Amendments Act, and 1.3% involved an unidentified authority. On the other hand, traditional investigative methods, including the use of tips, informants, intelligence from traditional CIA and FBI sources, routine law enforcement, militants' self-disclosure, and reports of suspicious activity initiated 60% of investigations. The initiation methods in 27.6% of cases are unclear; though possible, it is unlikely that NSA surveillance initiated these investigations, as the government would have then likely

indicated such key contributions in order to emphasize the benefit of its surveillance programs. Either way, these statistics are inconsistent with US officials' claims about the large role that bulk surveillance plays in counter-terrorism efforts (Bergen, Sterman, Schneider, and Cahall, 2014).

In fact, available evidence suggests that bulk collection is not necessary. During a Senate Judiciary Committee hearing in October 2013, NSA Director Alexander admitted that the bulk collection of American telephone metadata had only prevented one known terrorist attack in the US (United States Senate, 2013). In this case, the government used telephone metadata to connect San Diego cab driver Basaaly Moalin with al-Shabaab, an al-Qaeda affiliate. The FBI discovered that Moalin was in contact with al-Shabaab officials when he was caught providing $8,500 to an al-Shabaab affiliate. Though bulk collected metadata was apparently used, it is noteworthy that the FBI did not start investigating Moalin until two months after the NSA first provided a tip. Furthermore, this one case which US officials use to argue the necessity of mass data collection does not even illustrate a need for sweeping bulk collection of metadata, but rather the collection of metadata for communications in which one party is a known or highly suspected terrorist. Such a metadata collection method would also have sufficed in other investigations,

such as that of Najibullah Zazi. Zazi, who was planning to bomb the New York City subway system in 2009, was communicating with an email address known to belong to an al-Qaeda figure five months prior to the NSA's interception of Zazi's email (Bergen, Sterman, Schneider, and Cahall, 2014).

The failure to prevent the September 11th attacks despite the slew of warnings suggests that what intelligence agencies require is not more data, but better responsiveness and appropriate information-sharing within government.

We are often presented with a dichotomy that has the 2001 terrorist attacks on one side, and government surveillance on the other. However, US intelligence agencies were repeatedly informed of possible attacks by Osama bin Laden for several months leading up to the September 11th attacks. In the spring of 2001, top officials were briefed by reports indicating the existence and advancement of bin Laden's plans. These warnings continued through the summer with reports indicating continuing plans for bin Laden's attacks and imminent threats (Eichenwald, 2012, September 10). The failure to prevent the September 11th attacks despite the slew of warnings suggests that what intelligence agencies require is not more data, but better responsiveness and appropriate information-sharing within government.

Many people perceive mass government surveillance of individuals' communications and actions as intrusive and ultimately discomforting (CBC News, 2015, January 28). Surveillance advocates quickly dismiss such apprehensions with the phrase, "If you have nothing to hide, you have nothing to fear." But as computer security expert Bruce Schneier counters, the "nothing to hide" argument is built on a premise that "privacy is about hiding a wrong" (Schneier, 2006, May 18). Privacy does not necessitate misdeed, and is a valued right that provides citizens immense comfort and satisfaction. Thus, privacy is worth protecting.

Privacy does not necessitate misdeed, and is a valued right that provides citizens immense comfort and satisfaction.

More complications arise when intelligence agencies seek to interpret the massive datasets they have extracted. Innocent jokes or statements can be misinterpreted as terrorist threats when taken out of their proper context. For instance, a man named Joe Lipari spent two years fighting charges after he paraphrased a quote from the film *Fight Club*. The literal meaning of his statement seemed to threaten an Apple store, but in context, it was a harmless joke written without the intention of pursuing violent action (Booth, 2010, September 24). Due to the clandestine nature of government surveillance operations, it is difficult to precisely quantify the number of individuals

incorrectly deemed a threat and inconvenienced by false charges. However, the fundamental issue of context must be addressed. To more accurately interpret the information they receive, intelligence agencies must work to develop accurate data analysis programs while ensuring the products of algorithms are checked by humans, who have greater capacity to contextually evaluate statements, and determine the true level of threat posed.

Surveillance of those who have done nothing wrong can lead to unjust repercussions for the innocent.

It is simply not the case that government surveillance always allows illegal acts to be prevented or punished, and better protects innocent citizens. The effects of pervasive surveillance are much more ambiguous, and often negative. Throughout history, governments have targeted individuals based merely on ideological, political, or religious beliefs rather than evidence of criminal intent. For instance, during World War I, the precursor to the FBI, the Bureau of Investigation, spied on and sometimes prosecuted war critics, anti-draft activists, and pacifists. Intense and intrusive FBI monitoring also targeted the civil rights, feminist, and anti-Vietnam movements (Fischer, 2015). Considering this pattern of abuse, it is best to forego surveillance of the communications of an entire country's population in order to avoid unjust targeting.

The government's mass accumulation of telephony and Internet data is unnecessary for ensuring national security. Furthermore, surveillance of those who have done nothing wrong can lead to unjust repercussions for the innocent. Therefore, the scope of government surveillance should be limited to:

- Telephony and Internet metadata of communications, in which one party is a known or highly-suspected terrorist, or person of threat
- Content of telephony and Internet communications of persons demonstrated to have probable involvement in terrorist activity—for which a warrant must be granted
- CCTV cameras in public spaces (thus excluding inside residences, corporate offices, etc.)

Ultimately, some measure of government surveillance must be maintained to ensure national security. However, restrictions must limit the scope of information monitored to protect innocent individuals from unwarranted targeting, and repercussions. Surveillance is a powerful tool that can be abused by unfairly targeting citizens, or wielded responsibly to improve public safety. Only responsible oversight and restrictions on surveillance programs will promote the justice we seek. C

Javaria Mughal is currently a Grade 12 student at The Woodlands School. After graduation, she plans to study English and Economics.

REFERENCES

Associated Press (2015, May 7). US Appeals Court: NSA Phone Record Collection Is Illegal. *New York Times*. <http://www.nytimes.com/aponline/2015/05/07/us/ap-us-nsa-phone-records-aclu.html>, as of May 29, 2015.

Baker, Peter (2013, June 17). Obama Defends Authorization of Surveillance Programs. *New York Times*. <http://www.nytimes.com/2013/06/18/us/politics/obama-defends-authorization-of-surveillanceprograms.html>, as of November 17, 2015.

Bergen, Peter, David Sterman, Emily Schneider, and Bailey Cahall (2014). *Does NSA's Bulk Surveillance Programs Stop Terrorists?* New America Foundation (January). <https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf>, as of May 29, 2015.

Bilton, Nick (2013, July 16). The Pros and Cons of Surveillance Society. *New York Times*. <http://bits.blogs.nytimes.com/2013/07/16/the-pros-and-cons-of-a-surveillance-society/?_r=0>, as of May 29, 2015.

Booth, Robert (2010, September 24). Twitter Joke Trial Man's Bomb Threat was "Hyperbolic Banter". Guardian News and Media. <http://www.theguardian.com/uk/2010/sep/24/twitter-joke-trial-bomb-threat>, as of November 17, 2015.

CBC News (2015, January 28). Cyber Surveillance Worries Most Canadians: Privacy Czar's Poll. CBC News. <http://www.cbc.ca/news/canada/cyber-surveillance-worries-most-canadians-privacy-czar-s-poll-1.2934916>, as of November 17, 2015.

Condon, Stephanie (2013, June 12). Lawmakers Question Legal Basis for NSA Surveillance. *CBS News*. http://www.cbsnews.com/news/lawmakers-question-legal-basis-for-nsa-surveillance/ as of May 29, 2015.

Eichenwald, Kurt (2012, September 10). The Deafness before the Storm. *New York Times*, <http://www.nytimes.com/2012/09/11/opinion/the-bush-white-house-was-deaf-to-9-11-warnings.html>, as of November 18, 2015.

Fischer, Linda E. (2015). *Guilt by Expressive Association: Political Profiling, Surveillance, and the Privacy of Groups*. Arizona Law Review 46: 621-675. <http://www.arizonalawreview.org/pdf/46-4/46arizlrev621.pdf>, as of November 24, 2015.

Granick, Jeniffer Stisa, and Christopher Jon Sprigman (2013, June 27). The Criminal NSA. *New York Times*. <http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html>, as of Nov. 18, 2015.

Schneier, Bruce (2006, May 18). The Eternal Value of Privacy. *Wired*. <http://archive.wired.com/politics/security/commentary/securitymatters/2006/05/70886>, as of Oct. 5, 2015.

United States Congress (2013, June 18). House Select Intelligence Committee Holds Hearing on Disclosure of National Security Agency Surveillance Programs. Congressional Hearings. <http://fas.org/irp/congress/2013_hr/disclosure.pdf>, as of November 18, 2015.

United States Senate, Committee on Health, Education, Labor, and Pensions (2013). *Continued Oversight of the Foreign Intelligence Surveillance Act*. Hearing, video (October 2). <http://www.senate.gov/isvp/?comm=judiciary&type=live&filename=judiciary100213>, as of November 24, 2015.