**2017 CCCAF Scholarship Essay - Hunter J. Dempsey**

*In regard to National Security, should the Federal Government have the authority to direct private companies to relinquish personal data from their customers?*

April 15, 2013 began like any other school vacation day. With freedom from our responsibilities as busy high school sophomores, my friends and I decided to cheer on the Boston Marathon runners as they crossed the finish line on Boylston Street before getting lunch near Fenway Park. Little did we know that a few short hours after we left the area, two bombs would detonate, taking the lives of three innocent people and injuring hundreds more. Luckily, my friends and I were not directly affected by the Boston Marathon Bombing, but the cowardly actions of terrorists permanently altered the lives of hundreds of people on this day that Bostonians will never forget.

Unfortunately, the Boston Marathon Bombing is only one of many acts of terrorism that have occurred in the United States and around the world in the past two decades, from New York City on September 11, 2001 to Paris on November 13, 2015. As a result of these tragic attacks, it is imperative that the government has the authority to carry out effective anti-terrorism efforts in order to prevent similar events from happening in the future. As a means of strengthening national security, the government should have the authority to obtain personal data from the customers of private companies. In our modern world saturated with technology, personal data can provide the government with valuable insight into the intentions and motivations of those who pose a threat to our national security.

However, this does not mean that the government should have unlimited, random access to personal data. Rather, private companies should be required to relinquish the personal data of their customers when the government has a valid reason and legitimate purpose for requesting it. For example, suspicious activity demonstrated by a member of an FBI terrorist watch list or a warrant seeking the personal data of a criminal suspect are justified reasons for providing access to this data. Beyond evidence of suspicious criminal activity or a demonstrated risk to national security, however, it is reasonable for private companies to protect the privacy of individual customers.

Based on concerning statements he had made, Omar Mateen was placed on a terrorist watch list multiple times before he massacred forty-nine people in yet another horrific act of terrorism in Orlando, Florida on June 12, 2016. Tamerlan Tsarnaev was also on the radar of the government before his homemade bombs exploded at the Boston Marathon finish line just hours after I left that exact spot. If the government had the ability to more closely monitor the personal data of Mateen, Tsarnaev, and others, government officials may have been able to prevent these senseless attacks. Martin Richard, the youngest victim of the Boston Marathon Bombings, made a sign before his death that read “No More Hurting People, Peace.” We should do whatever it takes to make Martin’s wish a reality, which includes enabling the government to access personal data as a means of protecting our national security and safeguarding precious human lives.