2017 Essay Topic: “In regards to National Security, should the Federal Government have the authority to direct private companies to relinquish personal data from their customers?

The Balance between Privacy and National Security

 With the increasing power of information systems and the readily available mobile technology, people that pose threats to National Security are storing important and incriminating data on mobile devices and computers. Private companies around the globe are storing the personal data through cloud computing facilities such as the ones owned by Apple and Amazon corporations. Each private company therefore protects the data under the privacy policies, but the United States government, in cases regarding National Security of their citizens, are requesting to access the personal data of offenders. The Federal Government should have the authority to direct private companies to release personal, incriminating, data about offenders and their threats on the protection of the population.

 The San Bernardino terrorist attack, which occurred December 2, 2015, is an example of the nation’s debate of privacy and security. The perpetrator Syed Farook’s Apple cell phone was a topic of debate and a six-week legal battle between the US government and The Apple Corporation. The Federal Government requested that Apple release Farook’s data and aid in the access to the locked iPhone. Apple, who had previously aided the government and complied with search warrants under the All Writs Act of 1789, refused to hack into its own device in this particular case. Before the case was brought to court, the FBI was able to gain access into the phone and therefore dropped the case against Apple. Apple denied the government access into the phone, as they believed that the government would further demand access to financial, health, and locational data of its citizens. Due to Apple’s refusal to comply with the FBI, the Apple user’s privacy is still at jeopardy. The FBI discovered a breach in the iPhone’s security that other hackers may also take advantage of, but to have access in future cases, the US government is withholding the security flaw from Apple.

 Murder cases are also in question, asking how investigators look at the digital footprints people leave. In 2015, an Arkansas man’s Amazon Echo, a cloud-streaming recording and listening device, data was requested in an investigation of a murder. Amazon denied releasing the recorded data stating, "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course." Tech companies should comply with investigators and the US government if crimes have been committed and the evidence withheld in the devices may be incriminating.

 Privacy in technology is not a feasible endeavor and new laws and standards should be set to allow the government access to data if security of others is at stake. Nothing streamed over the internet, mobile devices, or in home “smart” applications are private from hackers and the companies are storing “private” data for undisclosed or unregulated amounts of time. The Federal Government should have access to private company’s data on request in extreme circumstances and use the data to keep the majority of the nation more secure.

Dillon, Nancy, and Sasha Goldstein. "FBI Has Gotten into IPhone Used by San Bernardino

Shooter." NY Daily News. Daily News, 28 Mar. 2016. Web. 24 Mar. 2017.

Selyukh, Alina. "As We Leave More Digital Tracks, Amazon Echo Factors In Murder

Investigation." NPR. NPR, 28 Dec. 2016. Web. 24 Mar. 2017.

Yadron, Danny. "San Bernardino IPhone: US Ends Apple Case after Accessing Data without

Assistance." The Guardian. Guardian News and Media, 29 Mar. 2016. Web. 24 Mar.

2017.