Eric Trahan

English 123

Assignment 2-2

7/7/2020

As a part of the coursework for English 123, the class will eventually be writing persuasive essays. Each module, we build upon our chosen topic, learning best practices and techniques to make the eventual essay more impactful. For this assignment, I am going to be following a writing plan to help gather my notes and thoughts on my chosen topic.

Sacrificing privacy for security is bad. Specifically, taking away someone else’s privacy and claiming it will make them more secure is wrong. I fully believe that everyone should have a clear and easy-to-understand choice when it comes to privacy vs. security. It should be optional and presented with a detailed description of what exactly is being done. As a cybersecurity professional, I will mostly be arguing from a cybersecurity standpoint. This greatly relates to my current profession and chosen degree.

Some possible key points for my argument are oppressive governments, criminals, and costs vs benefits:

1. Oppressive governments are notorious for controlling what the people of their nation say and do. This helps them maintain their image and stay in power. They have very little privacy since everything they do is monitored for “security threats”. There are methods to bypass these security controls, but they are complicated and require a decent amount of technical knowledge. Therefore, you have a group of people who cannot tell the world about the horrible things going on in their nation at the hand of their government. This is an extreme example of what happens when sacrificing privacy for security is left unchecked.
2. The more information these security controls gather about individuals, the more likely they are going to be targeted by criminals. As an ethical hacker myself, I know that nothing exists that is un-hackable, and that it would be only a matter of time before their wealth of information is stolen to be used maliciously. The more data you collect, the more lucrative you are to steal from. This almost makes the security gained from sacrificing privacy non-existent.
3. What are the actual benefits of the security gained from losing privacy? On October 25, 1979, Australia implemented the Telecommunications (Interception and Access) Act 1979 which required telecommunications companies to retain specific telecommunications data for at least two years. The security benefit from the act is allowing law enforcement to quickly build evidence and arrest suspects. The cost is involuntarily giving up privacy. There are some who say that the government is good and is using it for good purposes, so it should not be an issue. While this may be true, there is no way for every citizen to trust their government truly and completely, and nor should there be. This amount of private data aggregated should make many people uncomfortable and wary. In the future or even secretly happening now, individuals in the government could abuse their power or begin to turn more authoritarian, using that data for malicious purposes. The government turn into the criminals they used the data for in the first place. The benefits do not outweigh the costs.

I think my audience will likely be those uneducated in cybersecurity, such as those who are unaware that they are being monitored and tracked daily. One of the biggest challenges I will face is explaining the technical side in a manner that can be easily understood. Providing examples, using simple language, over-simplifying some things, providing resources for further understanding, and relating concepts to more commonly understood examples are some of the ways I will help the audience fully understand. Their ability to understand exactly what I am saying is crucial to persuading towards my argument.

My end goals are to raise awareness about privacy concerns, convince people to my side, and hopefully help prevent more invasive security measures from being implemented. This essay will need a lot of research and examples to back up my claims. While I easily speak from my experience, that will only take my argument so far. It is hard to trust someone you do not know, which is entirely my point about trusting government with too much of your personal data.

There are tons of articles about this topic. There is also plenty of data on arrests, internet traffic, privacy laws, etc… The main issue is finding enough data that can undeniably correlate without conducting a study of my own (which is a whole different mess that I do not want to tackle). Here is a list of a few articles that I like and may use for my essay:

1. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32006L0024>  
   This is a directive implemented by the EU in 2006. It was annulled in 2014, but it is a good example of how governments justify their invasion of privacy.
2. <https://www.legislation.gov.au/Details/C2017C00192>  
   An Australian act passed in 1979, but reviewed several times and updated in 2017, this is one of the older acts, and therefore will have a lot of data and information regarding it. I expect to find a lot of articles defending both sides of the act.
3. <https://www.bjs.gov/>  
   The Bureau of Justice Statistics will have a lot of data and information regarding crimes, and in this case, cyber crimes. While the invasion of privacy is used for attributing more than just cyber crimes, it’s currently the most I have to go off of. I’m sure with more research I can find more data regarding arrests made due to the data retention acts.
4. <https://www.hrw.org/world-report/2019/country-chapters/north-korea>  
   An article on North Korea’s oppression will prove key to my oppressive government point. North Korea is notorious for controlling and lying to their people. There are many other articles and even some defectors’ stories. Expect to see more of this in my essay!

Key points to provided resources:

1. Oppressive Governments:
   1. All the above-mentioned resources can be used to show how these laws can slowly be used more and more aggressively.
   2. #4 is especially relevant.
   3. I would like to find more data and resources regarding oppressive governments who silenced their people.
2. Criminals:
   1. There is a massive amount of public release statements where a company announced their customers’ data stolen by hackers. The above resources do not necessarily complement this key point (except for maybe #3), but it will not be hard to find evidence that does.
3. Costs vs Benefits:
   1. This one is a bit tricky. While all the above will speak on benefits, especially #3, I will have to work extra hard to accumulate information on the costs. I’m thinking about showing the actual costs of retaining the data and increases in arrests, then comparing it to before these laws went into effect and the amount of arrests made then. This will give me a good model to see if the costs are worth the increase in arrests. If plausible, I will give better recommendations to use that money for (the world can always use more mental health support!).

I think the strongest point of my argument is by far the oppressive government point. Not only are there more examples of this from the past, but there are also modern-day examples happening even now. This is something everyone can understand and most likely agree with, making it my strongest point. I should probably spend most of my time focusing on this versus the other key points. My concern is whether I should focus on this early on to draw the reader in, or if I should talk about it last to make a bigger impact at the end.