I certify that this submission is my
Original work and meets the Faculty's
Expectations of Originality

Christopher McArthur
40004257
ENCS 393 AA
June 18th, 2018

Security Versus Privacy

In the last two decades these two concepts have become seemingly polar opposites. How can we have the luxury to scroll a news feed without fear of our homes being taken with know no knowing the random thoughts that we google at 2am? It seems every piece of the online world, from the operating system, browser, internet service provides, the CSA, every single government agency, the NSA, the KGB, the destination website, and that nerd who send you a phony email that's been spying for your credit card information… Everyone has their hands in the proverbial cookie jar which is identic to your identity and all your personal information. Does this really help keep the country safe? Does this prevent school shootings from happening or other terrorist attacks? For precision the security concept discussed here is on a national level, no one claims spying on citizens is to prevent small crimes; "keeping Canadians safe from treats abroad or at home" is a good paraphrase which explains the idea. The other half of this discussion is privacy which will be focused on privacy of personal information; a prime example is the Cambridge Analytica scandal on the shoulders of Facebook who unknowingly gave away several hundreds of millions of identities away. The internet has become a tool for us to share, connect and communicate with others we are close to and those on the other side of the world, however its also been the tool for those who wish to do harm to others, giving them access to all information they might need to build a bomb. Many groups have organised and planned their attacks using encrypted chat groups, but these details used to only surface after the fact. Therefore, there is a need for some monitoring to identify those who pose a risk for committing violent acts, which implies some degree of spying on personal information. Yet everyone seems to be collecting your information and selling it to the anyone for market analysis. Why is everything about you available for sale online? Do we allow, or consent for this to happen? One can't help but wonder how much of our identity is owed by someone else? The link between governments protected its citizens through gathering information of the internet and internet companies tracking everything we do is from the laws the governments are putting emplace to allow themselves access also gives access to private interest.

So here we have it; whenever we access the internet everything we do is saved, tracked, and builds an identity of us but is this cost worth the level of protection to our home land security from attacks from within or abroad. It is very common for anything we say to pop up as an ad and its that in-depth knowledge of us that in the wrong hands could be very dangerous.

Judging the morality of this topic requires applying a formal theory of morality. Approaching this subject from a utilitarian point of view, we can judge the ethical issue by evaluating the outcome of pleasure from the position of an aggregate. For this thought exercise we will focus on Canadians who have a free high access to internet percentage and a very low number of terrorist incidents. First off, its very surprising despite every Facebook user agree to the terms and conditions for their information to be collected and owed by Facebook, very few Canadians know that's actually what's going on. It's mostly due to the cultural epidemic where not reading those conditions is normal. Since a large portion

have no clue what's going on, their level of pleasure is unaffected. This leaves a majority of the population aware of the privacy breach to various degree, however since it does not stop many people from using the internet it id safe to conclude the discomfort from having everything you do tracked is very minimal on average, but most would call it concerning or irritating. This discomfort while using internet services, which is often done as a distraction, for fear of missing out, or for social acceptance, diminishes the quantity of pleasure we derive from an activity many people spend several or tens of hours each day using. On the flip side of this are the lives saved from preventing terrorist attacks but how many lives are save? Do Canadians feel safer? Does this translate to pleasure? There are very few statistics on the number of incidences that are prevent from information gathering, the suspicious is that the disclosure would include the scale of the domestic spying. None the less there is no evidence to suggest that Canadians feel safer with all their personal information being saved in datacenters, in fact there is a small coefficient suggest we actually feel less safe, more at risk, with the possibility of loss of identity. This all sums up to a null-sum where any small gain of pleasure gained from the increase of security is negated by the decrease of pleasure which rises from the fear of identity theft. The end result is a large portion of the population who is displeased from the uncomforted with the vast amount of their information being kept by private companies. By this end result the utilitarian would classify the misuse of the internet to gather personal information is an immoral action because the compound effect on pleasure to those involved are negative.

The second way to judge the morality of this usage of this information and communication technology is through the lens of deontology and the formula of ends in itself. This methodology involves determining consent of all parties and whether or jot someone is being used as an end or just a mere means. Internet service companies and using the millions of people as a mere means to meet bottom lines by offer information to ad agencies. The more difficult quest is do Canadians consent to the gathering of their personal information. Using these websites like Facebook and google you agree to the services because you made an account or followed the hyperlink to the terms and conditions and agreed to all the legal garaging. The fact of the matter is you most likely didn't even notice the blue underlined text because you are so conditioned to clicking okay without knowing. If this was a bank loan or an important legal contract, would you have read and understand everything before signing your life away? Well surely you took the same seriousness when making your Facebook account. Or is it more likely giant tech companies have known for years and exploited this flaw of users not knowing what they are agreeing too to get away with much worse things then we have yet to find out? Arguable the strongest reasons why we put all of our information online if not for convince and relative ease, is the social pressure to not miss out on anything, to followers and to be liked. This social construction of our online profiles being an extension of us is often used to cover our flaws or change what we don't want to see in ourselves. We feel compelled and obliged to share everything and by merely using the service you consent to it collecting your information however how does this extend to the government collecting your information for a threat assessment? We elect our representatives and they on our behalf devise laws which are made to protect use and provides services which are too costly for any individual. Through this democratic system we have chosen to allow the government to put in place laws which allow all internet services to gather our information. Adding the issue of security, which arguable is part of the role of the government, most Canadians would agree that sacrificing some privacy such that every could bit a little bit safer is an acceptable compromise which further leads to the proof that we consent to our information be gathered. Through these optics, we have given companies the ability to gather our

information through accepting terms and conditions which we naively or ignorantly ignore. We are in favor of the government monitoring everyone for bolster our domestic security.

The next theory of morality to test the misuse of this technology is the justice for fairness model. This comprises of removing yourself from society and from the veil of ignorance or the original position enter into a world with this or these laws in place transition from the original position to any possible roll affected by the law with any possible trait. If you would enter into any position and accept this law than it is fair and justice. Applying this theory through a case study of the gathering of personal information through the internet we are faced with a world were everyone who connects is being monitored. Even those responsible for a large part of the private sectors who gather personal information for profit still put tape over the webcam and microphone of their portable devices. Its inescapable surround all of us. Worst of all you don't need to be online yourself for your data to be collect, especially with social media platforms after you have deleted your account, what those around you share or post can still be linked with your virtual data that they owe about you. There is a hard-deterministic relationship that occurs between society and the internet, there is a sentiment that the internet's momentum has taken over the world and whatever consequences a rise we are forced to deal with. It's the will of the Internet. Perhaps entering the society, you would be upset with how others can spy and gather your information, but ignorance in bliss and those actions are very seldomly advertised. So, under the veil of ignorance with no knowledge of the transgressions against you, you would be inclined to accept to live in this society. On the other hand, you could be one of the out spoken individuals who feels the attack on our privacy and personal lives, but these individuals almost never believe they can make any difference, they accept the reality that the internet can not be fought, that it the way it is, it certainly could be better but changing it, molding it to a shape better match for society is not possible. So, whether you are blissfully unaware or an outspoken advocate for change or just somewhere in the middle its very unlucky you would be against living in this society. Through this thought exercise we can accept the living in this this society with any trait therefor the laws are fair and just according to the acceptance criteria of our third theory of morality.

Through the various thought exercises applying three different theories of morality we have varying answers. The utilitarian would deem this misuse as immoral because it diminished the quantity of pleasure for a large portion for what is an hourly task for many. Using the fairness for justice model, entering a society from any position would no lead even the more aware and out-spoken advocate to reject to live in this society. Then in the middle what the deontology Formula of an End in Itself, where the using someone merely as a means to reach financial targets is unacceptable but having those you take advantage of given their constant either ignorantly, consciously or democratically does put this misuse in a neutral light. The technology on internet communication is highly compatible with democratic forms of governance however the technology of gathering information using internet communications for building profiles is necessarily militaristic, whereby you need absolute control over the nations infrastructure in order to control all the flow of information though dedicated agencies build for filtering through the petabytes of data the is transferred every second. With this in mind, how to we alleviate some of discomfort felt from the gathering of our personal information? We have seen people are willing to accept a diminished privacy for an increase in security and the gather of information will no let to the public rejecting the society. What is missing is the public engagement in science and technology, particularly internet communication technologies, where the majority have little to no understanding of the fundamental systems in place that build this global infrastructure. Including the

public regarding the finer details of what is acceptable to be gathered, how it can be gathered, what measures must be taken to keep that information safe and most importantly what it can be used for. Once the public feels it has control over something that is misunderstands it can regain some faith I the major internet service companies that have come so ingrained into our vocabulary and daily lives.