Mannkal Economic Education Foundation

Economics Scholars Essay Competition

Question: Should governments be able to access personal information from social media websites such as Twitter and Facebook? Is it ever appropriate for governments to close the Internet and mobile phone networks?

Name: Robert Joseph Chasland

The possibility of government monitoring of social networking sites such as Facebook and Twitter is one of the greatest threats to self-determination and liberty in the modern era. Indeed, any proposed government control of the internet should be fought tooth and nail – *savior c'est pouvoir* – knowledge is power, and the internet is this generation's means of sharing information; of communication. To remove the greatest protection of communication, *anonymity*, would render all private conversations open, a concept no one should be comfortable with.

Policies of monitoring the internet are manifesting themselves around the world, becoming well established in the United States and Europe in the last decade. However, the risk of these same policies spreading to Australia is very real.

This is predominantly an issue that dominates the most avid of internet users - the youth. Since the Greens movements of the sixties and seventies, the environment and sustainability were the major concerns of the young. However, recent surveys have shown that these values have been displaced and that the single biggest anxiety of worldwide youth today is internet privacy.

And it's not just the young; the 'X generation' is concerned also. Tens of thousands of people protested throughout Europe concerning the European Data Retention Directive, tabled in the European Union Parliament in 2006; a directive which both monitors any internet or phone use and makes phone companies record user's phone use. The information derived from the phones and web are then stored from 6 months to two years. Despite the wide opposition, the Data Retention Directive was tabled.

In the 5 years since this Data Retention directive, the Pirate Party – a protest party formed in response to this directive – has become the fastest growing political party in history and now has representation in over 59 countries. This growth demonstrates the avid opposition worldwide to introducing any type of internet control.

However, the internet and its explosion in the last two decades seem to have rendered many politicians out of touch with these sentiments. Politicians are humans, not monsters, and they in the most part are trying to further society, and in these endeavours try to protect us. But in this case they are misguided, it seems likely that if parliamentarians were told that by monitoring the internet and social networking sites, they were in essence placing a surveillance bug on every desk in the country, they would most likely be horrified. Our lawmakers need to understand that if they legislated to monitor the interent, they would be overstepping their duties as representatives – showing they are out of touch with majority public sentiment.

Society today just wants to enjoy the privileges that society forty years ago enjoyed – that communication was private and anonymous. The analogy of Facebook and Twitter electronic messaging to mail is a strong and appropriate one. Forty years ago, if you sent a letter, you had the choice to put the sender's identity on the outside of the envelope, on the letter or not at all, and the government had no right to look inside the envelope to find out. All society today wants is those same rights to translate to today's form of mail, albeit an electronic form.

Despite Facebook being a public forum, no one has the intention of having the government reading what it is posted there, nor should it even be in contemplation – it is entirely unnecessary.

In the countries where internet monitoring has been introduced, the excuses have all been different - terrorism, organised crime, most excuses concerning public safety - has always

had the same outcome – internet monitoring. Should society have to sacrifice more self determination to satisfy public safety? It seems ludicrous that people privately messaging the contents of their last meals should be monitored in order to uphold public safety. Indeed, though the contents of my last meal aren't the most important of information, I would still be uncomfortable with the government having possession of such personal, albeit trivial information.

However, what would happen if the government was handed control of the internet? Allowed access to our Facebook and Twitter accounts? Looking at countries that have this legislation are startling.

In the Egyptian uprising of early 2011, when the protests were at their heaviest, President of Egypt and Dictator Hosni Mubarack switched off the internet in an attempt to break down the communication between protest leaders. Indeed with just a mobile phone a person could send a 'tweet' and start a protest. Luckily, the uprising was still successful, but Mubarack's actions speak volumes of the government's fear of the power of open and easy communication.

But even some Western '*civilised'* countries can demonstrate the disquieting possibilities. The Data Retention Directive of the European Union is just as scary, as a German citizen of the European Union, Malte Spitz found out. After reading about the directive, Spitz decided to investigate how much information the phone companies held. His phone company Duetsche Telecom (the biggest at the time) in Germany, when asked, reluctantly provided Spitz with 35, 830 lines of information just from the last 6 months, each line a minute by minute guide to his life, pertaining to a phone call, or a GPS tracking of his movements. Every citizen of the European Union who has a mobile phone has the same lengths of code – raw data tracking every call, every movement stored by their phone company. A simple mathematical program can then group the information, revealing who he called, who his friends called, and from there work out intricate detail such as leaders in the friendship group, when they go to sleep, when they go to work and so on. If you live in Europe, your phone company is protocoling your life for your government. It must not be allowed to happen in Australia, as these possibilities are startling.

Imagine the government who released the Data Retention Directive was that of East Germany of 1989, just before the Berlin Wall collapsed. Imagine that the thousands of people who protested and eventually tore down the wall had a mobile phone in their pockets. With the information that the phone companies could provide, the Stazi (East German Secret Police) could have found the leaders of the protests, had them murdered - they could have completely dismantled the protests before they even began. The fall of the Iron Curtain may have been completely prevented.

We cannot let this happen in Australia. Australian Federal and State Parliaments need to know that society wants self-determination in the digital age, and that living in the digital age and privacy render no contradiction. To stop this, society must realise that autonomy must be fought for; that privacy is necessary in the 21st century, is not an out dated concept, and it should be protected from government interference.