INTERNET ANONYMITY

The debate over Internet Anonymity has intensified over the years, and has culminated with the nymwars (2011)- the name given to the conflict between social networks and their users over the use of real names.

When the word ‘anonymity’ first appeared in the English language in the early nineteenth century, it was used to describe authors or writings that were not known by name (Ferry, A., 2002). Over the last three centuries the use of anonymity has dramatically changed as activists and writers have now begun to use nameless e-mails, Internet blog posts and social networks as platforms to influence audiences without being detected. While this use of pseudonyms and fake online identities has been historically policed efficiently, the last decade has seen an increasing rate of cyber-crime resulting from Internet anonymity. Despite the argument from many that maintaining Internet anonymity is in line with the freedom of speech component of the Universal Declaration of Human Rights, I will argue that there is a need to do away with the use of fake identities on the Internet. This paper will first highlight the emergence of the cyber – space as a political and social sphere that has become a breeding ground for terrorism. Subsequently, it will emphasize difficulty associated with policing the Internet by shedding light on various cyber-crimes that continue to harm our society. Finally, the paper will propose a solution that could possibly tackle the problems associated with Internet anonymity, while remaining cognizant of an individual’s right to privacy and free speech.

In order to establish a case against Internet anonymity, it is important to first understand the role of cyber – space in the world today. In her book titled “Cybering
Democracy: Public Space and the Internet”, Diana Sacco acknowledges that that the Internet has evolved from an information channel to a social and political space (Saco, D., 2002). The internet has served as a medium of social communication since 1997, when Six Degrees was launched as an online platform that allowed users to interact with their friends, family and acquaintances. Since then, a rapidly increasing global Internet subscriber base has paved the way for the creation of similar websites like Friendster, MySpace, Orkut, Google Plus and finally Facebook – a website with almost one billion registered users. Each of these websites has enabled individuals to network with their friends online through both private and public messages, photographs and videos. Having accepted that social networking websites provide users with the platform to continuously interact with each other, it is fair to classify the Internet as a social space.

Following this acceptance of the Internet as a social space, we can now proceed to examine how interactions in this social setting have had political repercussions across multiple countries. Prior to the discovery of the Internet, political activists regularly used newspapers, magazines and physical gatherings to promote their agenda. The common thread amongst every political movement from the Civil Rights movement to the Indian freedom struggle is the successful use of channels of communication to influence society. Social networking websites have succeeded in creating a virtual society that transcends geographical borders. This has opened up a plethora of possibilities to political activists that are trying to spread their message around the world. It is the presence of websites like Facebook, Twitter and YouTube that has led to the overnight emergence of “Kony 2012” – a documentary that highlights the atrocities committed by Joseph Kony, a Ugandan warlord.
As we go a little further back in time, it can be argued that the Arab Spring that has seen the citizens of Egypt, Libya and Syria pressing for democratization would not have been possible without the existence of the Internet. Philip Howard, a professor in communications at Harvard University noted that people who shared an interest in democracy used social media as a medium of mobilization. The value of social networks was highlighted by an average of 2,000 politics-related tweets per day in the Arab region for a period of two weeks following the start of the revolution in Egypt. The presence of blogging websites like Word Press and Blogger has further facilitated these political movements, thereby confirming that the Internet is a medium of political exchange and debate.

Having established that cyber–space serves as a social and political networking platform, I will now highlight the difficulties that are associated with the effective governance of this space. Law and order in traditional societies is facilitated by the fact that each member of society has a physical presence. Governance is made possible by the fact that thieves, murderers and other violators of the law can be physically tracked down by policeman. Further, it is this embodiment of the members of a society that binds them to their geographic location, and makes their behavior easy to supervise. However, the identity of this member is made complex within the cyber–space, where an individual can take on multiple identities without being recognized. Michel Foucault, a famous social commentator, acknowledged this difficulty when he asked what happened to politics and governance within the context of cyber–society, where ‘bodies’ were only made visible occasionally, and the primary method of communication was via writing (Saco, 2002).
The fact that ‘netizens’, or citizens of the cyber – space are difficult to govern is further compounded by Internet anonymity, which not only denies authorities a physical presence by which to identify offenders, but also an authorized legal name or address by which to track them down. While proponents of such Internet encryption will argue that anonymity allows people to enjoy their basic right of freedom of speech and expression while maintaining a sense of privacy, it may be argued that there is a distinct difference between privacy and anonymity. The right to not have one’s private information disclosed to unknown individuals or organizations is something that an individual should not be denied. However, it is dangerous for this definition of the right to privacy to include the freedom to not reveal one’s true identity to those that one chooses to initiate communication with.

The paper will now highlight the various dangers that are associated with Internet anonymity, while also proposing a possible framework for the governance of Internet users.

The presence of terrorist groups on the Internet is a relatively new phenomenon, but one that has exploded into life over the last decade. The terrorist attacks of September 11th, 2001 are considered one of the worst in recent history, and brutally exposed the western world to the changing face of terrorism. While the attacks remain notorious for the use of airplanes as missiles that can cause mass damage, it is important to note that 9/11 was the first major terrorist event to take place after the dot com bubble (1995-2000), which had awakened the world to the Internet and its various uses. Over the course of the
decade that has elapsed since 9/11, terrorist groups have regularly been reported to exploit blogging websites and social networks to promote their own cause. The perils of the Internet as a platform for terrorist activity have been highlighted by the noted researcher Dr. Maura Conway, who stated that every computer that is connected to the Internet is “potentially a printing press, a broadcasting station or a place of assembly.” Terrorist groups appear to be well aware of this, and it is evidenced by the fact that the Liberation Tigers of Tamil Eelam used the Internet to publish pictures of the Air Tiger Squadron just a few days before it conducted an aerial attack on the Sri Lankan government facilities. The online distribution of the beheading of American journalist Daniel Pearl is further proof that the terrorists have begun to use the cyber – space as a medium to promote their propaganda. The advantage that terrorists have by using the Internet is that they can engage in activity without revealing their identities and this makes it difficult to track them down.

In addition to promoting propaganda, Internet anonymity is being increasingly used to plan and co-ordinate attacks. One of the last e – mails that was extracted from the account of Mohammed Atta, one of the perpetrators of the 9/11 attacks read as follows – “The semester begins in three more weeks. We’ve obtained 19 confirmations for studies in the faculty of law, faculty of urban planning, faculty of fine arts and the faculty of engineering”. When decoded, this e mail is believed to be in reference to the three major targets of the Al Qaeda, which were the World Trade Centre (faculty of engineering), the Pentagon (faculty of fine arts) and the Capitol building (faculty of law). Unfortunately, due to the encrypted nature of the e mail, and Atta’s practice of using anonymous e-mail
accounts, security agencies were unable to interpret and prevent the attacks beforehand. The use of anonymous e-mail accounts has indeed become a common practice in modern terrorism (Source: International Telecommunications Union). In order to communicate, one terrorist creates a web-based e-mail address under a false name or pseudonym and shares the user name and password with the rest of his accomplices. The terrorist types out the instructions that he wishes to send in the format of an e-mail, and instead of sending the e-mail, simply saves it as a draft. The rest of his accomplices can then log into this account from their remote locations read the draft and delete it immediately. The next day, a new account is used for the same practice, and in this manner terrorist groups are able to successfully orchestrate attacks without being tracked by authorities.

While terrorism is possibly the most dangerous threat that is posed by cyber – space encryption, there exists a plethora of cyber – crime possibilities that can arise due to the protection of Internet anonymity. Internet fraud refers to the use of the Internet to defraud individuals by stealing their private information and even their identities. This form of fraud has been prevalent ever since the Internet was first launched and has continued to remain a popular method for criminals. In 2004, the FBI reported that they had intercepted more than 3,700 counterfeit postal money orders that could be sourced to the Internet between October and December of that year. The frequency of such activities has increased over the years, with individuals using a number of different platforms on the Internet including e-mail spam, work at home schemes, and money transfer fraud. The fraud associated with e-mail spam alone is estimated to be more than $250 million over the last year, and authorities have since admitted that such activity is facilitated by the fact that
individuals can generate these schemes while keeping their legal names and addresses a secret.

Finally, the Internet is also home to millions of blogs and message chat boards and online communities. These can be accessed by almost every Internet user, and while a vast majority of them are relatively harmless, there do exist a large number of such websites that are associated with topics like white supremacy, homophobia and the aiding/abetting of suicide. For example, a basic google search containing the words “white supremacist group” provides users with more than five million search results, the first twenty of which, are direct links to supremacist groups online.

The content on these websites is generated by users that mask their real identities in order to prevent detection, and leading personalities in the legal sphere have acknowledged the problems that are associated with policing this cyber-space. In a recently concluded panel discussion on Internet anonymity, Dean Saul Levmore of the University of Chicago noted that while objectionable content on television or in magazines and newspapers can be regulated by legal authorities, it is impossible to do the same for the Internet due to the fact that messages are posted anonymously, and Internet Service Providers (ISPs) refuse to divulge the legal names that are associated with IP addresses.

With the Internet opening up extremely realistic possibilities of terrorism, fraud and other criminal activities, there is an urgent need to devise a solution that effectively deals with the perils of Internet anonymity while still protecting an individual’s right to privacy.
and free expression. In a report compiled by an Internet security research group, the use of the blocking lists was put forth as a possible mechanism that protects against the dangers of Internet anonymity (Callanan, Gercke, De Marco and Dries–Ziekenheiner, 2009). The primary purpose of Internet blocking would be to screen and block any objectionable online content from being displayed in the cyber–space. This has already been in practice for a number of years via e–mail filters and private firewalls. However, a strategy that protects against Internet anonymity would require a much larger scale strategy. Perhaps the most pertinent question that is associated with the use of blocking lists is deciding which content is dangerous and which is not.

While traditional practices of blocking involve the pre-emptive creation of an automated list that contains all words and images that are objectionable, this practice unlikely to work on a larger scale since it would create too many restrictions and possibly screen out a significant amount of content that actually is not harmful. Instead, authorities should put into place a neutral organization that scans potentially harmful content on the Internet (which will be brought to its attention by the filters put in place by a blocking list), and blocks anything that is perceived to harm society as a whole. Understandably, the greatest challenge to such a problem would be to agree upon an organization that is neutral. However, it is possible to set up such organizations in countries where the judiciary is independent from the executive arm of the political system. This appears to be the case in a number of democratic countries, and the solution would then be to create a self-governing screening body that comprises of members of the judiciary, which is tasked with the responsibility of identifying any online content that could lead to terrorist or other
cyber-crime activity. A similar independent body comprising of members of the judiciary has been created in the European Union to curb corruption, and has met with relative success. Ivan Bizjak, Director General for Justice and Home Affairs in the European Union has acknowledged the organization’s effectiveness by stating that the fight against graft would not have been made possible without the presence of a body that is free of political and lobbyist interferences. The proposed organization that is responsible for the removal of harmful content on the Internet can be structured similarly and be programmed to avoid the influence of other government officials.

As websites and social networks continue to develop platforms that facilitate communication, the threats of cyber-terrorism, Internet fraud and other forms of cyber-crime is ever-present and evolving. As with most forms of technology, there is a learning process involved, and strategies to combat the problems associated with Internet anonymity are likely to advance over time. While the solution proposed in this paper is not something that should be considered for countries that do not have democratic systems in place, I believe that the successful implementation of an autonomous Internet screening agency in a country with an independent judiciary will go a long way in combating the problems that are associated with anonymity in cyber-space.