THE JUSTIFIABILITY OF STATE SURVEILLANCE OF INTERNET COMMUNICATIONS AS AN E-SECURITY MECHANISM

Murdoch Watney

Professor: Faculty of Law, University of Johannesburg

mmw@regte.rau.ac.za

(011) 489-2027

Private Bag 524

Auckland Park

2006

ABSTRACT

The purpose of this paper is to investigate the legal justifiability of measures contained in state surveillance laws pertaining to the Internet.

Prior to the terrorist attack on the United States of America (U.S.) on 11 September 2001, the concept 'surveillance' was nothing new and is indeed as old as human society. As far back as the sixteenth century the first central state surveillance appeared in Britain.

The commercialization of the Internet and computer-related technology replaced the industrial society with an information-based society and contributed to globalization. The Internet brought about many advantages but at the same time unlocked several challenges unknown to the physical world. Internet-connected countries battle to control the flow of information across borders for the purpose of national security and law enforcement. State surveillance of the Internet is utilized in addressing the abuse of the Internet, such as the commission of organized crime and terrorism.

The 9/11 terrorist attacks coupled with the effect of globalization reinforced and accelerated the use of technology-based surveillance which includes state surveillance of electronic communications in the U.S. Many countries have since followed suit and introduced legislation providing for state surveillance of Internet communications by means of interception, monitoring, data retention and decryption.

The western world has always jealously guarded the protection of human rights, yet new technological and political developments often challenge the human rights culture. The exploitation of the Internet for the commission of serious crimes challenges countries to find ways of controlling cyberspace, whilst at the same time encouraging the continuous growth of the Internet, stimulating technological innovation and enjoying the benefits of the Internet.

KEY WORDS

State surveillance; Internet; legislation; legal regulation; justifiability; e-security; law enforcement; national security; globalization

THE JUSTIFIABILITY OF STATE SURVEILLANCE OF INTERNET COMMUNICATIONS AS AN E-SECURITY MECHANISM

1 Introduction

The term 'surveillance' evokes the concept of 'big brother' as created by George Orwell. Many South Africans would however rather associate it with the television reality show 'Big Brother' where the daily actions of a group of people living in a house was under constant video surveillance and broadcasted to television viewers. The connotation is not wrong. 'Surveillance' given its broadest meaning, means 'to watch over'.

On a more academic note, the 'big brother' that George Orwell so fearfully described in his book, *1984*, was the coming into existence of a state-controlled central surveillance system (Lyon, 1994:57; 2003:29; Bowrey, 2005:81). Little did Orwell in 1948 foresee the present society: a society dependent on information existing in a globalized world. The Internet is but one of the factors contributing to globalization but in view of the major effect it had on countries, it requires closer investigation. The justifiability of state surveillance is discussed within the context of Orwell's 'big brother'.

The inherent characteristics of the Internet namely a faceless, borderless, many-to-many, 7 days a week 24 hour access and transfer of information within cyberspace, contributed to globalization. Although the Internet brought many advantages, it also unlocked challenges that had hitherto been unknown in the physical world.

Countries have looked for answers in addressing the challenges posed by the Internet ever since its implementation. One of the solutions has been state surveillance of the Internet. It would be erroneous to argue that the debate regarding the merits of state surveillance laws of the Internet has become unnecessary as a result of the implementation of the Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002 (hereafter referred to as the RIC Act) in South Africa and the surveillance laws of the European Union (EU), especially the Directive on mandatory data retention. Despite the implementation of state surveillance laws, most countries including South Africa, are still in the initial phase of given effect thereto. The constitutionality of state surveillance laws will most probably still be challenged in court.

The central question of this paper concerns itself with the justifiability of state surveillance laws of Internet communications as an e-security mechanism. As legal regulation is a certainty, the question of justifiability concerns itself with the content of the laws, or differently put, what is and should be regulated.

An evaluation of the justifiability of Internet state surveillance laws can only take place once the following issues have been investigated, namely:

i. the relationship between surveillance and security;

ii. the impact of the Internet on countries;

iii. the global effect of the US terrorist attack on 11 September 2001;

iv. the legal position regarding state surveillance laws in the EU, the U.S. and South Africa; and

v. an overview of some considerations in respect of the regulation of state surveillance of the Internet.

It should be noted that state surveillance of the Internet is not only of interest to the information and communication technology professional and lawyer, but all users of Internet services. Many may erroneously be of the opinion that state surveillance is exclusively a legal and technical issue, however state surveillance of the Internet has ethical, political, economic and sociological consequences.

2 'Surveillance' and security

The term 'surveillance' is often used without clearly indicating which category of surveillance, type of surveillance or surveillance method is applicable. 'Surveillance' is an umbrella term that encompasses different categories of surveillance, different types of surveillance in each category and different surveillance methods. This discussion will focus on the category, state surveillance, the type of state surveillance is the Internet pertaining to surveillance methods such as monitoring, interception, data retention and encryption.

Security involves the use of technology for the protection of information and communication technology. State surveillance, within the context it is used here, means the gathering of information regarding unlawful conduct such as for example, websites canvassing support for terrorist activities, money laundering and organized crime.

State surveillance of the Internet for the purposes of law enforcement and national security is a security mechanism enabled by technology. Not all categories of surveillance will be e-security mechanisms for example, customer surveillance resulting in customer profiling for marketing purposes. The question arises whether the purpose of state surveillance of the Internet justifies for example human rights violation?

3 Impact of the Internet on countries

The Internet contributed to globalization. Globalization within the context of the Internet pertains to the borderless and unrestricted flow of information between countries. Access to blogsites, websites and secure communications can be gained from anywhere in the Internet connected world.

Dependence on Internet services has grown exponentially. The negative aspect to this dependence is vulnerability to abuse of the Internet. During November 2005, delegates from 174 countries attended the World Summit on the Information Society (WSIS) in Tunis and decided that one of its main focus areas would be expanding worldwide access to information and communication technology by 2015 and at the same time protecting the free flow of information, ideas and information. This means that more people would in future enjoy the benefits of the Internet, but at the same time, the negative consequences of globalization by means of the Internet will increase.

The negative aspect of globalization centres on the impact the Internet has on the role of individual countries and sovereignty. Countries that previously had control over the lives of their citizens within the national borders, now battle to exert control over information from across borders. Countries have no control over the nature and content of the Internet, for example a website set up by extremists for purposes of propaganda and obtaining financial aid. Organized crime and money laundering are in some instances used to aid terrorism. Crimes are now international for example in many instances phishing syndicates operate from outside the borders of a country. The phishing syndicate sends e-mails to unsuspecting Internet users requesting for example, bank particulars that the user, oblivious to the security risk, supplies. 'Runners' then transfer the money into their account and then again into the bank account of the syndicate

(Computer crime research centre, 2005:1). It is clear that countries need control over the Internet to ensure security of the Internet and to ensure trust and confidence in the use of the Internet.

Furthermore, the Internet as a new 'form' of power is acknowledged by the use of state surveillance (Bowrey, 2005:178, 174 – 175). Examples are the setting up of 'gripe' websites such as "neverflysaa", environmentalists protesting against whale hunting in Japan and the defacement of U.S. websites expressing dismay with globalization and capitalism.

The Internet as an international tool was not created with security as a primary consideration, but as a communication and information tool (Vatis, 2001:8). Countries realized that the negative impact of the Internet had to be dealt with without minimizing its benefits. One of the solutions was state surveillance as an e-security mechanism, not only by means of surveillance technology, but also legal regulation of the use of surveillance technology. The nature of surveillance technology such as impersonal, automated, non-obvious but invasive, intrusive and extensive surveillance needs legal regulation setting out the parameters and safeguards to the development and use of surveillance technology.

Acknowledging that surveillance technology needs legal regulation brings another problem to the fore, namely 'legal' governance of the Internet. Since the Internet is not a single entity, but an interconnected system of networks, the question is who determines the legal regulation of the development and use of the Internet. This question is closely linked to state surveillance laws of the Internet. A global Internet cannot be regulated within national borders alone as information comes from outside the national borders. It therefore implies that a country such as South Africa has to follow a legal comparative approach to Internet laws and consider international Internet laws in determining its own laws. It appears that the EU and the U.S. would be the main 'powers' when it comes to prescribing legal regulation of the Internet. Most countries in the world have for example adopted the EU data protection regime. The EU and U.S. therefore strongly influence state surveillance laws of the Internet worldwide.

4 Global effect of the 9/11 US terrorist attack

A discussion of surveillance must be conducted against the background of the terrorist attacks on the U.S. on 11 September 2001, as this event was a watershed between the past and future of surveillance (Edwards and Howells in Nicoll, Prins and Van Dellen, 2003:237). Although surveillance had existed prior to 9/11, a consequence of the U.S. terrorist attacks was the intensifying and reinforcement of surveillance by means of the use of technology (Lyon, 2003:6).

The 9/11 attacks were an international event of cataclysmic proportions that set in motion various processes (Lyon, 2003:132). Bearing in mind the international influence of the U.S, 9/11 triggered a renewed worldwide focus on the combat against terrorism. A few days after the US terrorist attack the UN Security Council adopted Resolution 1373 on 28 September 2001. This Resolution obliges States to take all kinds of measures aimed at the prevention of terrorist acts and at the bringing to justice of those who participated in the financing, planning, preparation or perpetration of such acts or in supporting them (Wouters and Naert in Fijnaut, Wouters and Naert, 2004:138).

Involved in the U.S. terrorist attacks had been air traffic, foreign nationals and networked messages and therefore airline passenger data, immigration records, telephone and e-mail logs became the focus of surveillance. The U.S. attack was not only organized from within the U.S. national border but soon after 11 September, it became known that the attacks had been prepared in part in Western Europe, particularly in Germany (Fijnaut, Wouters and Naert, 2004:5). 11 September highlighted the issue of security in a globalized world.

Consequent to the 9/11 U.S. terrorist attacks, there have been the Madrid bombings in 2004 and the United Kingdom (UK) bombings in 2005. It is a given today that terrorism is not confined

to a specific country but that it is rather an international issue. International cooperation is essential in addressing international terrorism. Regarding international cooperation, the two dominant worldwide forces are the U.S. and EU. The EU has strongly supported the US in its initial reaction to 9/11 and has extended cooperation to the U.S. It is also interesting to note that the events of 9/11 provided an incentive to the EU to have a more unified approach to international terrorism and for the EU and U.S. to overcome the obstacles regarding international criminal law experienced prior to 9/11 (Wouters and Naert in Fijnaut, Wouters and Naert, 2004:139-140).

5 Overview of state surveillance laws of the Internet

5.1 Introduction to Internet state surveillance laws

Countries can only control the Internet for law enforcement and national security purposes by employing state surveillance technology governed by means of legal regulation. These laws should be seen against the background of 9/11. Already as far back as 1997 at a meeting of the Justice and Interior Ministers of the G8 countries held in Washington DC, it was emphasized that international co-operation and mutual assistance are essential regarding cyber crime. Internet laws of the different countries must be harmonised, otherwise cyber criminals exploit the discrepancies between different criminal justice systems and loopholes in international criminal law to their advantage, resulting in many perpetrators escaping prosecution (Schloenhardt, 2005:121). Countries must therefore put aside sovereignty in ensuring criminal justice in cyberspace. Internet state surveillance laws will have to reflect a uniform approach.

5.2 Council of Europe Convention on Cybercrime

The Council of Europe is an international organization that plays an important role in shaping the criminal policy of EU member states and in strengthening international cooperation against crime. The Convention on Cybercrime of the Council of Europe is the only international treaty regarding cyber crime. The Convention on Cybercrime recognizes that the investigation methods retaining to physical crime cannot effectively be applied to cyber crime and it therefore outline procedural methods specifically aimed at the collection of evidence for the detection and investigation of cyber crime. The Convention on Cybercrime provides for surveillance methods such as interception and preservation (not retention) of data but only with regard to data of identified perpetrators regarding specific crimes.

The Convention on Cybercrime requires that countries have an ability to implement interception of data either with the assistance of internet service providers (ISPs) or in circumstances where there is no service provider or where the service provider is not able to provide assistance to be able to exercise these powers themselves. The latter power is necessary because the Convention only requires providers to provide assistance within their technical ability. In a serious case where law enforcement has obtained an interception order but the service provider lacks the ability to assist them, law enforcement requires the ability to implement the terms of the order itself, otherwise critical evidence may be lost. The Convention on Cybercrime does not require any particular architecture or technical capability to intercept data. Articles 20 and 21 of the Convention on Cybercrime state that an ISP need only collect data within its existing technical capability when ordered to compel data through proper legal process.

The Council of Europe accedes that the meaning of ‘interception’ is problematic. The Council of Europe suggests that the procedure of interception be distinguished from the procedure of search by looking at the state the information is in, namely whether the information is in transit or inert (Carr in Nicoll, Prins and Van Dellen, 2003:197-206). Interception would be applicable to data moving between computers or storage files whereas the search procedure would be applicable to

static information stored in one machine or one file store (Carr in Nicoll, Prins and Van Dellen, 2003:199).

The Convention on Cybercrime empowers enforcement authorities to search computer systems and seize information, order service providers within its jurisdiction to provide information in respect of the subscriber such as identity, postal address, billing and payment information, collect traffic data in real time and ask others such as service providers to assist in this collection and interception of content data. The Convention on Cybercrime provides for the request of preservation and disclosure of stored data and provides for data preservation for a period of up to a maximum of 90 days.

There is no mandatory data retention obligation in the Convention on Cybercrime. There is a data preservation provision. It is important to distinguish between data retention and data preservation. Data retention requires providers to collect and keep all or a large portion of its traffic as a routine matter. Preservation of data on the other hand enables law enforcement authorities during the course of a criminal investigation to instruct a service provider to set aside specified data that is already in the service provider's possession until the necessary authorization for disclosure has been obtained. The ISP is obligated only to preserve data that it is currently storing, if requested to do so by a law enforcement agency with respect to specified data in a particular case.

The procedural law applies to traffic data as well as content data. The Convention on Cybercrime defines 'traffic data' as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

5.3 European Union

On 14 December 2005 the EU adopted the Data Retention Directive that provides for mandatory data retention of Internet communications between 6 to 24 months although EU member states may extend the retention period. EU member states have 18 months from the date of the adoption of the directive to incorporate this mandatory data retention provisions into the member state's legal system. The Directive does not limit data retention to terrorism and organized crime but includes all serious crimes as defined by each individual member state. It covers what is known as 'traffic data'.

Mandatory data retention as a method of surveillance must be seen against the background of the:

i. European Convention of Human Rights and Fundamental Freedoms (hereafter referred to as ECHR) of 1950;

ii. Council of Europe Convention on Cybercrime of 2001;

iii. two data protection directives, namely the Data Protection Directive 95/48 EC regarding the processing of personal data and free flow of information in general, and the Privacy and Electronic Communications Directive 2002/58 EC in respect of processing of personal data within the ambit of an electronic medium; and

iv. European Union Declaration in Combating Terrorism adopted in 2004.

EU Directives must be adopted by the EU member states as national law taking into account the circumstances, culture and history of the member state. The national adoption of the mandatory Data Retention directives may be tested in national courts if it is in breach of citizens' human rights. In respect of the EU, it can also be taken to the European Court of Human Rights.

According the general Directive 95/46/EC and the specific requirements of Directive 2002/58/EC for the processing of personal data and the protection of privacy in an electronic

communication medium, 'traffic data' must be erased or made anonymous when it is not needed for the purpose of transmission or necessary for billing purposes. The primary purpose of processing traffic data is to technically enable users, who are at a physical distance from each other to communicate (Walden in Nicoll, Prins, Van Dellen, 2003:152-153). Prior to the Data Retention Directive, article 15 of Directive 2002/58/EC provided EU member states with a data retention measure for a limited period of time if it is a "necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system." It also states that the retention of data should be in accordance with the European Convention on Human Rights and Fundamental Freedoms as interpreted by the rulings of the European Court of Human Rights. The Mandatory Data Retention Directive has now amended article 15 and provides for compulsory data retention of traffic data of all Internet users.

Article 8(1) of the ECHR provides: "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8(1) is subject to article 8(2) of the ECHR that states: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."

5.4 United States of America

After 9/11, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act) was implemented. The USA Patriot Act is not a single coherent law, but the act collected hundreds of minor amendments to federal law, grouped into ten subparts or titles on various topics. Relevant is title II that provides for enhanced surveillance procedures that expand intelligence and law enforcement capability to identify and investigate terrorist activities and includes provision that among other things enhance law enforcement surveillance abilities (Raul and Tyler, 2006:9). The USA Patriot Act distinguishes between direct surveillance where the surveillance is undertaken by the government using its own technology on the network of a service provider, for example the FBI's carnivore and indirect surveillance where the service provider is requested to provide information.

It appears that Internet privacy in the U.S. does not derive from the Constitution but legislation such as the Electronic Communications Privacy Act of 1986. The courts have held that an individual has no reasonable expectation of privacy in information revealed to third parties, for example, an Internet user cannot enjoy a reasonable expectation of privacy in non-content information sent to an Internet Service Provider (ISP) because the user has disclosed the information to the ISP. The U.S. courts have held that in general the Internet user has a reasonable expectation of privacy in content information that is sealed away from the network provider but does not retain such protection in information disclosed or openly visible to the provider (Kerr, 2003:627-630).

Recently much opposition have been levelled against the USA Patriot Act regarding human rights violations. It is interesting to note that the US does not make provision for mandatory data retention of all users as the EU, but only for the preservation of data similar to that of the Convention of Europe. Some have suggested that the EU surveillance laws with specific reference to data retention goes much further than the U.S.

5.5 South Africa

South Africa provides in the Regulation of the Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (hereafter referred to as the RIC Act) for state surveillance of the Internet for law enforcement and national security purposes such as crime prevention, detection and investigation. The crimes are defined in a schedule to the act and provides for serious crimes such as terrorism, fraud and money laundering. The RIC Act came into operation in September 2005. A directive regarding technical and practical issues were passed in November giving the ISP 6 months to implement the interception and data retention capabilities.

The RIC Act must be seen against the background of section 14 (right to privacy), section 16 (right to freedom of expression), section 36 (limitation clause) and chapter 11 (government must ensure state security) of the Constitution.

The RIC Act provides for indirect surveillance which means that the Internet Service Provider will carry out surveillance on behalf of law enforcement agencies such as the police. The ISP must have the following two capacities, namely:

i. Interception of indirect communications. The RIC Act does not refer to Internet communications but to indirect communications. Indirect communications is defined as the transmission of information by means of an ISP; and

ii. Storage of communication-related information. Traffic data is referred to as communication-related information. 'Communication-related information' refers to the information in the records of the ISP and includes information regarding the switching, dialling and signalling which identifies the origin, destination, duration, termination, time, date, size and type of service used.

Interception relates to part or whole of the content of Internet communications. The general rule is that no indirect communications may be intercepted. There are however exceptions to the general rule such as interception by means of an interception directive. 'Interception' is understood to mean the acquisition of parts or whole of the contents of indirect communications and include the listening to or recording (monitoring), viewing, examination and inspection of the indirect communication and also the diverting of the indirect communication to an interception centre. Interception will occur during the transmission of the information, meaning while the information is in transit between computers or storage files and it includes the storage of indirect communications, such as an e-mail for later retrieval or usage. The indirect communication is intercepted by someone other than the sender or recipient or prospective recipient.

Besides interception of the content, the ISP must store communication-related information for a period of three years. This is a blanket data retention obligation. As indicated, communication-related information (traffic data) is divided into two categories, namely real-time communication-related information and archived communication-related information. Real-time communication-related information is immediately available to the ISP before, for or during a period of 90 days since the transmission of the indirect communication. Archived communication information is in the possession of the ISP and in storage beginning on the first day after the expiration of the 90 days since the transmission of the indirect communication. The general rule is that the ISP or an employee may not disclose communication-related information unless with the authorization of the subscriber. However, the RIC Act provides for exceptions to the general non-disclosure rule by means of a real-time communication-related direction, archived communication-related direction and an encryption direction.

South Africa adheres to some of the provisions of the Convention on Cybercrime as the RIC Act for example provides for interception and encryption. The data retention or storage of communication-related information is however not the same as that proposed by the Convention on Cybercrime.

6 Some considerations in respect of justifiability of state surveillance laws of the Internet

6.1 Introduction

In paragraph 5 the international as well as South African surveillance laws were discussed. It is however important to scrutinize the justifiability of state surveillance laws. As indicated, the Internet is a global information and communication medium and therefore national laws must be harmonized with international laws or else the legal regulation of the Internet will not be effective. Consideration should be given to some aspects of state surveillance of the Internet.

6.2 Considerations

6.2.1 It would be erroneous to consider state surveillance as only a technical and legal issue without giving any regard to the political, sociological, economic and ethical implications of this concept. One of the criticisms has been that it results in racial profiling due to the nature of the surveillance technology, namely the use of algorithm.

6.2.2 State surveillance laws reflect the changing role of the ISP. It was initially stated in the Electronic Communications and Transactions Act 25 of 2002 that the ISP does not have an obligation to monitor. It soon became clear to the legislator that the successful enforcement of legislation in cyberspace was dependent on assistance from the ISP. A good example would be the amendment of the Films and Publications Act 65 of 1996 to the effect that it is now required that the ISP must register with the Films and Publications Board and also block access to child pornography. Regarding state surveillance laws the ECT Act provides for indirect state surveillance, meaning that the ISP must assist in the surveillance on behalf of intelligence agencies and law enforcement agencies. An ISP may experience this legal burden as cumbersome, especially in light of the fact that this has nothing to do with its main function, namely as a conduit of information.

6.2.3 Data retention has evoked a lot of discussion and will continue to do so. Most countries are in the process to implement such data retention legislation. As indicated, in the US only a preservation order is applicable but following the EU, many countries will implement a mandatory data retention of all users. The following aspects regarding mandatory data retention should be taken into consideration:

a. ISPs will have to secure the stored information and will have to employ security measures to avoid unauthorized access to the stored data.

b. The period of data retention will vary between countries. In South Africa it is 3 years whereas the EU has proposed a maximum period of 2 years. The Internet is however under constant change and it is an open question whether the data will still be relevant after 2 years, taking into account that the Internet changes a lot and websites as well as IP address may be obsolete after a period of 2 years.

c. It may from a technical perspective, not be easy to distinguish between traffic data and content data. In practice, content and traffic data are often generated simultaneously resulting not only in revealing data which is necessary for the conveyance of an electronic communication (namely traffic data) but which also shows elements of the content indicating the interests of the user.

d. Various debatable questions may be raised such as why the traffic data of all Internet users need to be stored as it results in a human right infringement. Can the human rights violation be justified by the positive effect it has in combating terrorism and preventing the commission of serious crimes?

e. The question is often posed why we need traffic data for law enforcement or security intelligence purposes. Traffic data may provide the only clues to the identity of the

perpetrator, although nearly all forms of traffic data may be altered or masked by sophisticated criminals. Every piece of traffic data may be described as a piece of jigsaw puzzle and the more data there are to cross check, the harder will it be to put the law enforcement agencies on the wrong track.

f. Data retention laws are pro-active policing. This means that it aims at addressing the security risk or the crime commission risk before it is actually committed. This is commendable as policing is normally reactive. It addresses the crime once it has been committed. The question remains whether intelligence agencies and law enforcement agencies will be able to identity a threat before its actual commission.

6.2.4 George Orwell feared an integrated central state surveillance. State surveillance of the Internet today is much wider than Orwell's feared central state surveillance, but an integrated global state surveillance system is emerging.

6.2.5 One should also distinguish between state surveillance and censorship as practiced by China. Censorship is an example of ultra-regulation and unlike state surveillance of the Internet, affects the free flow of information.

6.2.6 The final word on surveillance laws has not yet been spoken. Surveillance laws may still be challenged in national constitutional courts and regarding EU member states, it may also be challenged in the European Court of Human rights.

7 Conclusion

It is no wonder that some has referred to state surveillance as a pandora's box, since it is a complex topic that involves many inter-related issues. It is also clear that governments walk a tightrope in balancing the aims of state surveillance of the Internet with justifying human rights violations. Citizens will have to debate the use of surveillance technology and laws to prevent a country moving from a surveillance state to a police state. It should be borne in mind that technology is changing constantly and may render surveillance technology so extensive that it would be difficult for legislation to keep up with ensuring protection of its citizens. However, in a globalizing and ever-changing world, governments have little choice but to make use of surveillance technology regulated by laws.

No one is denying the role that surveillance has to play, but the question is how far surveillance should be allowed to go. The remark by former US president, James Madison, is in this regard relevant (Taylor, 1987:118): "If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the Government to control the governed; and in the next place, oblige it to control itself." Indeed wise words that governments and its citizens should heed.

7 References

Books:

Bowrey, K. 2005. *Law and Internet cultures*.

Carr, I. 2003. "Anonymity, the Internet and Criminal Law Issues" in Nicoll; Prins and Van Dellen,. *Digital anonymity and the law*.197 – 206.

Fijnaut, C; Wouters, J and Naert, F. 2004 *Legal instruments in the fight against international terrorism.*

Lyon, D. 1994. *The electronic eye: the rise of surveillance society.*

Lyon, D. 2003. *Surveillance after September 11*.

Taylor, L.B. 1987. *Electronic surveillance*.

General Web-based documents:

Computer crime research centre. 2005. Phishing details. [Online]. Available www.crime-research.org/news/29.07.2005/1394/ (Accessed 8 August 2005).

Raul, A.C and Tyler A. L. 2006. The USA Patriot Act of 2001: electronic surveillance and privacy [Online]. Available www.sidley.com/cyberlaw/features/patrot.asp?print=yes (Accessed 7 February 2006).

Vatis, M.A. 2001. Cyber terrorism: the state of US preparedness. [Online]. Available www.ists.dartmouth.edu/ISTS/counterterrorism/preparedness.htm (Accessed 2 November 2002).

Legislation:

European Union:

Directives 95/46/EC and 2002/58/EC

European Convention of Human Rights and Fundamental Freedoms (ECHR) of 1950;

United States of America:

*The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Ac*t of 2001 (USA Patriot Act)

South Africa:

Constitution of South Africa 108 of 2002

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

Paper-based journals:

Kerr, O.S. 2003. "Internet surveillance law after the USA Patriot Act: the big brother that isn't". *Northwestern University Law Review*, 627-630.

Schloenhardt, A. 2005. "Transnational organised crime and the international criminal court developments and debates". *University of Queensland Law Journal* 93-121.