UNDERSTANDING ELECTRONIC SURVEILLANCE AS AN INVESTIGATORY METHOD IN CONDUCTING CRIMINAL INVESTIGATIONS ON THE INTERNET

*Murdoch Watney

Abstract
Cybercrime undoubtedly threatens the global growth and future of the Internet. Governments cannot ignore the abuse of the Internet and must address cybercrime that includes terrorism, cyberwar and iWar. Many governments have elected to utilize electronic surveillance as an investigatory method in addressing the prevention, detection, investigation and prosecution of crime in an electronic medium such as the Internet.

The emphasis in this paper will be on facilitating an understanding of the legal regulation of the use of Internet surveillance as an investigatory method bearing in mind that surveillance is made possible by means of technology. The central question will be why and how do governments provide for surveillance as an investigatory method in addressing criminal investigations on the Internet. The approach to the discussion will be from a global legal perspective without addressing a specific country's Internet surveillance laws.

Criminal and intelligence investigations in most countries face the same dilemma: how can a crime on the Internet be investigated in the pursuit of criminal justice whilst maintaining a human rights culture and preventing governments becoming police states with all Internet users seen as guilty until proven innocent. It is a dilemma that requires all stakeholders to carefully monitor the implementation of surveillance and specifically, the surveillance methods, in criminal and intelligence investigations conducted on the Internet.

1. Introduction

Crime is as old as mankind itself. However, as society evolve the type of crimes and the methodology of crime commission change.[1] Criminal investigation has to keep abreast with these changes to ensure the apprehension of perpetrators and institution of criminal trials.

Law and specifically the laws[2] governing the criminal justice system traditionally developed in a physical world. Prior to the development and implementation of the

---

* Professor of Law at the University of Johannesburg, South Africa.

1 Van der Merwe "Computer crime –recent national and international developments" 2003 *THRHR* on 32 refers to Tapper *The third wave* (1981) who identifies three "waves" (phases) of development, namely the agricultural, industrial and information phases which affect crime commission.

2 The criminal justice system comprises of criminal law, law of criminal procedure and law of evidence. The law of evidence is divided into strict and free system of evidence; see n 5.

computing technology and the Internet, there were many developments that brought with it advantages and disadvantages, such as providing new tools for the commission of crime. In most instances, the 'traditional' laws governing the criminal justice system were flexible enough to accommodate the investigation of crimes resulting from these 'new' technologies.

The biggest challenge to the 'traditional' laws governing the criminal justice system resulted from the decision of the United States of America (USA) in 1992 to commercialize the Internet. The commercialization of the Internet had many far-reaching consequences, some not anticipated by the USA or the Internet-connected countries.[3] Most of the consequences impact on and challenges the 'traditional' laws governing criminal investigations[4] and intelligence gathering.[5]

Governments have elected to use electronic surveillance as an investigatory method on the Internet. Electronic surveillance,[6] specifically in respect of the Internet, is an aspect that fascinates many (including me) and although much have been written on it, each author approaches it from a different perspective.[7] Surveillance is a wide topic that covers many inter-related aspects. In this paper the focus will be on the motivation for and justifiability of the use of electronic surveillance as an investigatory method on the Internet[8] in respect of criminal investigations and intelligence gathering of serious crimes on the Internet, such as terrorism, organized crime and money laundering. The emphasis is not on the collection, analysis and presentation of electronic information[9] as electronic evidence[10] in a court of law, although the information should be collected in such a

---

3 See Watney "The Evolution of Internet Legal regulation in addressing Crime and Terrorism" 2007 *Proceedings of the Conference on Digital Forensics, Security and Digital Forensics* 19 – 29 for a discussion of the consequences; also see par 3 hereafter.

4 Criminal investigation is defined as the gathering of evidence that can be used in a court of law to prove a crime has been committed. The investigation of crime may involve various investigatory methods such as the search of a premises and seizure of objects and taking statements of witnesses.

5 Intelligence gathering would be defined as the gathering of information that is in the interest of national security in a criminal investigation.

6 Electronic surveillance is made possible by means of technology and the purpose of surveillance is the collection of electronic information; see par 4 for a definition of the term, surveillance.

7 Lyon *Surveillance after September 11* (2003); O'Harrow *No place to hide* (2006).

8 The Internet is defined in the South African Electronic Communications and Transactions Act 25 of 2002 as an "interconnected system of networks that connect computers around the world using the Transmission Control Protocol (TCP) and Internet Protocol (IP)."

9 In this paper the term 'electronic information' will be used. It is important to distinguish between electronic information and data. Nieman *Search and Seizure, Production and Preservation of Electronic Evidence* (2006 thesis North West University) on 29: "Information is the end product of data processing. … In other words information has exclusive meaning for human beings, as opposed to data which is meant as instructions for a computer.

10 Schwikkard, Skeen and Van der Merwe *Principles of Evidence* (1997) on 6: "There exist basically two systems of evidence: the Anglo-American (or so-called strict or common law) system and the Continental (or so-called free or civil law system). The South African law of evidence belongs to the Anglo-American "family". Most of the principles of the Anglo-American law of evidence stem from the English system of adversarial (accusatorial) trails before a lay jury as opposed to the Continental inquisitorial trials by professional judges adjudicating without the assistance of a true

manner that it would be admissible in a court of law. The paper highlights the risks inherent to state surveillance and how it can be counteracted. It demonstrates how technological changes in the way we communicate today, influence investigations of crimes.

2 Criminal investigations in a physical and an electronic medium

2.1 Introduction

The laws governing the criminal justice system developed in a physical world and the question arises whether the 'traditional' laws can accommodate the electronic medium (also referred to as 'cyberspace'[11]) or whether the 'traditional laws' should be adapted to the electronic medium or whether new laws should be implemented? A meaningful answer can only be provided once the criminal investigations in a physical medium (so called 'real space') have been compared with that of an electronic medium (so called cyberspace).

One must be careful not to overstate the differences between the two mediums, but it is important to realize that criminal investigations in cyberspace provide challenges unknown to the investigations in a physical medium and an in-depth discussion of the differences is required.

2.2 Criminal investigations in a physical medium

The laws governing criminal investigations and the investigative methodology employed were developed for a physical medium and may be characterized as follows:

a. The object of the crime is mostly tangible in nature;
b. The main perpetrator is physically present during the commission of the crime;
c. Crime is predominantly investigated within the borders of a country and jurisdiction as well as choice of laws is seldom issues of dispute. Countries mostly have territorial control regarding the investigation of a crime within a physical medium;
d. Law enforcement agencies conduct criminal investigation and ensure enforcement of law;
e. The traditional procedural approach to criminal investigation and including the investigatory methods, is predominantly re-active: once the crime has been committed and brought to the attention of the law enforcement agency, an investigation commences; and
f. The criminal and procedural law is aimed at the prevention and investigation of a crime resulting in a prosecution.

---

jury." In the civil system the judge is not guided by rules of admissibility but the determination of weight attached to the evidence.

[11] William Gibson popularized the term, 'cyberspace' in his 1984 novel, *Neuromancer*. It denotes the place where communications on the Internet takes place. The Internet (see n 8 for a definition of the Internet) and cyberspace are sometimes used as if they are one concept, but they are different concepts with different meanings.

2.3 Criminal investigations on the Internet or differently put, cyberspace

The commercialization of the Internet and specifically the introduction of the World Wide Web (WWW) in 1995, resulted in the rapid integration of the Internet into global society. The Internet present several challenges to the characteristics of the traditional criminal justice system, such as

i. The use of computing technology introduced a new medium, namely an electronic medium that co-exist today with the physical medium. The Internet expanded the electronic medium to include a global borderless 24 hour 7 days a week communication and information system;

ii. It introduced the information age that evolves around the generation, exchange, receipt and storage of information, an intangible object. Any crime[12] committed on the Internet (electronic medium) is in respect of information. The investigation of cybercrime involves the gathering of information or differently put, electronic evidence. In 2003 a South African author, Van der Merwe,[13] remarked: "As the information revolution continues to gather speed, the criminal law has had to resort to an ever greater amount of tricks and sleight of hand in order to maintain the impression that it can cope with the protection of information." In this discussion attention will focus on how the criminal justice systems of countries in 2008 address the protection of information on the Internet against crime;

iii. The Internet caused conduct prohibited in the physical world, so-called traditional crimes such as child pornography, fraud and"identity theft" to move to an electronic environment. Many of these traditional crimes can be affected quicker, faster and in some instances, with more serious consequences, within an electronic medium. The Internet also introduced new methods of criminal abuse of the Internet that had not existed prior to the implementation of the Internet, so-called Internet crimes such as denial of service and hacking. Initially some countries did not specifically criminalize this conduct but it could also not be accommodated under the definitions of the traditional crimes. The non-regulation of the so-called Internet crimes resulted in legal uncertainty;

iv. Cyber crimes are committed without the physical presence of the perpetrator at the time and place of commission of the crime. Where more than one perpetrator is involved, it is possible for the perpetrators to communicate online without meeting face-to-face. The crime can also be committed against more than one victim.[14] One-on-one victimization is not typical of cybercrime, as cybercrime can

---

12 There does not exist a uniform definition of cyber crime. Van der Merwe "Information technology crime – a new paradigm is needed" 2007 *THRHR* on 311 argues that one should rather speak of information technology crime than cyber crime. For purposes of this discussion, cyber crime is defined as the use of a computer either as the object of the crime or the instrument of the crime or incidental to the crime. The crime evolves around electronic information and is made possible by means of computer technology.

13 "Computer Crime" 2003 *THRHR* 33. Van der Merwe used the different era's of human development again in an article, "Information technology crime – a new paradigm is needed" 2007 *THRHR* 311.

14 Nieman *Search and Seizure, Production and Preservation of Electronic Evidence* (2006 thesis North West University) on 3: "One-on-one victimization is not typical of cybercrime, because

be automated, unlike real world crime. With automation, perpetrators can commit thousands of crimes quickly and with little effort and one-to-many victimization could be seen as the default assumption of cybercrime;[15]

v. The nature of the Internet is one of many factors that contributed to globalization.[16] Globalization is characterized by conduct that is increasingly being done at a distance.[17] The terrorist attack on the US on 11 September 2001 (referred to as 9/11) was made possible by means of globalization;[18] and

vi. Although the Internet introduced an information and communication medium that facilitates the commission of crime any time from anywhere in the world, the activities take place somewhere and virtual spaces are downloaded and accessed in particular places in the physical world. It is therefore clear that although an Internet user has borderless access to the Internet, the crime originates from a place in the real world and the result thereof are experienced in a place in the real world. It is also possible to link the crime to a person in the real world. Investigators can establish the identity of the perpetrator by means of investigating the information (data) available on the Internet. If a crime originates from outside the borders of a country for example money laundering or a paedophile syndicate, the investigators have to rely on international assistance and co-operation in gathering and sharing the information.

From these challenges the following problems regarding the investigation of cybercrime are identified:

a. Some countries have inadequate criminal and procedural laws to detect, prevent, investigate and prosecute cybercrime. Even if a country regulates conduct on the Internet within its territory, crimes may be committed from outside the country's borders and originate from a country that does not regulate Internet conduct or enforce such regulation. It is therefore important to have an international treaty on

---

unlike real world crime it can be automated. With automation, perpetrators can commit thousands of crimes quickly and with little effort and one to many victimization could be seen as the default assumption of cybercrime."

15 Nieman *Search and Seizure, Production and Preservation of Electronic Evidence* (2006 thesis North West University) 3.

16 Larry *Globalization and Everyday Life* (2007) on 7: "Globalization is essentially about transnational flows (of people, money, cultures, goods etc.) across borders, but its effects will always be spatially located somewhere and virtual spaces are downloaded and accessed in particular places." Lyon *Surveillance after September 11* (2003) at 111: "The free flows of technology, persons, data, images, pests, information, waste ides, and, now terrorist networks that both constitute and characterize globalization are very hard to slow down or to stop. The world of the internet, with its built-in capacity to seek ways around obstacles and to continue working even when some nodes are taken out, typifies these global flows."

17 Lyon *Surveillance after September 11* (2003) 110.

18 Larry *Globalization and Everyday Life* (2007) on 182: "It is ironic that the ability for global terrorism to strike at large numbers of countries simultaneously was facilitated by globalization and has now become its biggest challenge." Lyon *Surveillance after September* 11 (2007) at 110: "September 11 and its aftermath has everything to do with globalization, which both enabled the event to happen and provides the conduits for its consequences." Fijnaut, Wouters, Naert (ed) *Legal Instruments in the fight against international terrorism A Transatlantic Dialogue* (2004) at 5: "Quite soon after 11 September, it became clear that the attacks were prepared in part in Western Europe, particularly in Germany."

cybercrime, which regulate the collection of evidence in respect of criminal investigations. If Internet-connected countries ascribe to such an international treaty, one will have harmonized criminal and procedural laws in respect of criminal investigations;

b. Crime investigators must act quickly as the electronic trail may otherwise go cold. Inadequate foreign co-operation and assistance in investigating international crimes and sharing of evidence result in investigators not being able to locate the criminal.[19] The Council of Europe realized that an international treaty can go a long way in assisting foreign co-operation and assistance. It was responsible for the implementation of the only international treaty, the Convention on Cybercrime.[20]

c. Although the emphasis in this chapter is on the collection of information by means of surveillance and not on the admissibility and reliability of the evidence, the criminal procedural laws and/or laws of evidence of Internet-connected countries must address the admissibility and reliability of such evidence;

d. As indicated, the traditional procedural approach to law enforcement has been re-active. This approach is not successful in the detection and prevention of crime. As terrorism is an ongoing threat to some countries it is important that information is gathered to detect and prevent such attacks;

e. A law enforcement agency cannot effectively investigate a crime on the Internet without the direct or indirect assistance of a third party, namely the Internet Service Provider (ISP). The evolution of Internet legal regulation in addressing crime, highlights the changed role of the ISP as a mere conduit of information;

f. Compliance with legislation within an electronic medium is not easy to enforce. For example in most countries the distribution of, access to and possession of Internet child pornography is prohibited but who ensures compliance? The question arises whether the ISP should carry this obligation; and

g. Information and communication technology is ever evolving. Investigators must not only keep up with the technological changes, but also have the necessary technical ability and skills to investigate cybercrime and gather information. It is also important that the law governing criminal investigations is flexible enough to accommodate technological development.

3. Motivation for the use of electronic surveillance on the Internet

The evolution of Internet legal regulation[21] illustrates the motivation and reasons for the use of electronic surveillance as an investigatory method in obtaining information available on the Internet.

The evolution of Internet legal regulation in addressing crime makes for interesting and in some instances controversial, reading. It illustrates how governments grapple with

---

19 Nieman *Search and Seizure, Production and Preservation of Electronic Evidence* (2006 thesis North West University) 4.

20 See par 5 for a brief discussion of the Convention on Cybercrime.

21 Watney "The Evolution of Internet Legal regulation in addressing Crime and Terrorism" 2007 *Proceedings of the Conference on Digital Forensics, Security and Digital Forensics* 19 – 29.

finding solutions to address crime committed in an electronic medium such as the Internet but at the same time try to uphold a balance between security and protection of human rights. It also illustrates that the laws governing the investigation of a crime in a physical world cannot merely be applied to an electronic medium, since the electronic medium has its own unique character.[22]

The following three phases are identified and summarized:

First phase: no governmental regulation of the Internet. When the USA commercialized the Internet, the US government was of the opinion that the Internet community could regulate the Internet themselves. Although the release of the first worm, the Morris worm in 1988 (prior to the commercialization of the Internet) challenged the concept of self-regulation, the 'I love you' virus released in 2000, forced Internet-connected countries to realize that the Internet community had grown so exponentially since the commercialization of the Internet that self-regulation could not successfully address criminal behaviour.[23]

Second phase: conduct regulation. Although conduct regulation resulted in criminalizing conduct such as the release of a virus and worm, launching a denial of service attack, it did not address the investigation of the crime. For example conduct regulation does not address the enforcement of the prohibition on Internet child pornography? 'Identity theft' (fraud) is and continues to be a big problem. In most instances, by the time that the victim discovers that he/she is the victim of 'identity theft' the evidence needed to establish the identity of the perpetrator does not exist anymore. The latter example illustrates the problem experienced with the re-active procedural approach to criminal investigations in a physical world.

Third phase: extending conduct regulation to include the control of information by means of electronic surveillance for the purpose of criminal investigation. Prior to 9/11, countries realized that conduct regulation only addressed the criminal law, but the investigation of crimes and specifically the traditional investigatory methods were not effective in an electronic medium. Countries needed a solution to address criminal investigations on the Internet.

The solution sought had to comply with pre-requisites such as that it had to assist, not only with the prevention and investigation of crime such as 'identity theft' but also with the detection of crimes such as the use of the Internet for inciting terrorism and furthermore, it had to address the problems experienced with investigations in an electronic medium.

---

22 Nieman *Search and Seizure, Production and Preservation of Electronic Evidence* (2006 thesis North West University) on 9: "The challenges posed by cybercrime cannot be solved merely slapping existing criminal and criminal procedural laws which govern the physical world onto cyberspace."

23 Here reference should be made to the South African government that initially did not regulate conduct on the Internet. The non-regulation of conduct from the period of 1993 (commercialization of the Internet in South Africa) to August 2002 resulted in legal uncertainty.

The 9/11 USA terrorist attacks on the World Trade Centre and Pentagon was not only a world event, but it was also a globalized event.[24] It impacted throughout the world. The 9/11 USA terrorist attack and the ongoing terrorist activities in Europe have had a globalizing effect on the laws governing surveillance 9/11. It served as a catalyst to move onto the next phase of development, namely electronic surveillance. Surveillance prior to 9/11 as an investigatory method existed but after 9/11 electronic surveillance was intensified and law enforcement and intelligence agencies powers were extended.

4. Understanding the meaning of the concept 'surveillance' as an investigatory method on the internet

Before referring to the surveillance laws of other countries that govern criminal investigations on the Internet, it is important to understand what is meant with the term 'surveillance' and whether there exist any international treaty in respect of Internet surveillance that can serve as a benchmark.

'Surveillance' means in its broadest "to watch over." Information gathering by means of electronic surveillance can be conducted by means of the use of non-communication devices such as biometrics, RFID and video cameras. In respect of communication devices such as the cell phone and the Internet, the information has to be gathered on the communication medium.

'Surveillance' of the Internet is an umbrella term that refers to the collection of different types of information on the Internet by means of surveillance methods (or procedures). The aim of electronic surveillance conducted on the Internet is the gathering (collection) of electronic information (evidence) to investigate a serious crime (which includes terrorism and terrorism-related activities). The surveillance methods are procedures used to ensure access to and availability of information on the Internet and must be distinguished from other information gathering methods such as search and seizure. Since Internet surveillance is invasive, it is limited to serious crimes and terrorism.

When investigating a crime on the Internet, investigators seek the collection of the following types[25] of information:

i. Content data: Content information is the equivalent of a letter inside an envelope.[26] Content data is not defined in the international treaty on Cybercrime but it is understood as the meaning or purport of the communication or the

---

24 Lyon *Surveillance after September 11* (2003) 109.

25 Berkowitz "Packet Sniffers and Privacy: why the No-Suspicion-Required Standard in the USA Patriot Act is Unconstitutional" 2002 *Computer Law Review and Technology Journal* on 2 distinguishes between traffic and content data as follows: "In thinking about electronic surveillance, it is important to distinguish between two kinds of information that the government might seek. One is addressing and routing information, equivalent to what one could learn from reading the outside of a sealed mail envelope without being allowed to open." and "The other type of information is content information or the equivalent of the letter inside the envelope."

26 Berkowitz "Packet Sniffers and Privacy: why the No-Suspicion-Required Standard in the USA Patriot Act is Unconstitutional" 2002 *Computer Law Review and Technology Journal* 2.

message or information being conveyed by the communication.[27] The collection of content data is also perceived as more invasive as collecting traffic data.

ii. Traffic data: Traffic data is the addressing and routing information, equivalent to what one would learn from reading the outside of a sealed mail envelope without being allowed to open it whereas content information is the equivalent of the letter inside the envelope.[28] Traffic data is information that is automatically generated when a criminal uses the Internet and can be useful to those investigating crime as it is similar to the physical DNA or fingerprints that are left at a physical crime scene. Although there does not exist a uniform definition for traffic data, most of the definitions have similarities, such as traffic data refers to data indicating the origin, destination, duration, termination, the size of the communication or that traffic data refers to the records kept by the ISPS when a user engages in online activity.[29] The Convention on Cybercrime[30] 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.

When investigating a crime that involves the Internet, investigators will determine the applicable surveillance method by looking at the type of information they wish to gather.

Investigators gather content or traffic data by employing the following different surveillance methods:

i. Interception;[31]

---

27 S 1 of the South African legislation, Regulation of the Interception of Communications and Provision of Communication-related Information Act 70 of 2002 defines content data "when used with respect to any communication, includes any information concerning the substance purport or meaning of that communication."

28 Berkowitz "Packet Sniffers and Privacy: why the No-Suspicion-Required Standard in the USA Patriot Act is Unconstitutional" 2002 *Computer Law Review and Technology Journal* 2.

29 S 1 of the South African legislation, Regulation of the Interception of Communications and Provision of Communication-related Information Act 70 of 2002 does not use the term 'traffic data' but communication-related information which is defined as "any information relating to an indirect communication which is available in the records of a telecommunication service provider and includes switching, dialing or signaling information that identifies the origin, destination, termination, duration, and equipment used in respect of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such telecommunication service provider and, where applicable, the location of the user within the telecommunication system."

30 The Convention on Cybercrime will be discussed at par 5.

31 Interception is defined in s 1 of the Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002 as "the aural or other acquisition of the contents of any communications through the use of any means, including an interception device so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the –

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any indirect communications; and

(c) diversion of any indirect communication from its intended destination to any other destination. It is obtained in the course of its transmission and can be obtained on an ongoing

ii. Monitoring;[32]
iii. Traffic data retention[33] or preservation of data;[34] and
iv. Data decryption.[35]

The surveillance method used will depend on the type of information required and the format of the information at the time of gathering. The information (content and traffic data) on the Internet may be collected either by the ISP (indirect surveillance) or by the investigating agency (direct surveillance).

Interception and monitoring is applicable to obtaining content information that is fluid and in movement at the time of gathering. The content is gathered during the transmission of the communication. Interception relies on a suspicion in advance of a criminal act.

The collection and 'storage' of traffic data is aimed at traffic data that is static, recorded and stored at the time of the gathering. Traffic data may be stored either by means of traffic data retention or traffic data preservation. In many countries data retention or data preservation is a new legal procedure or power that never existed in the physical medium. The ISPs in some countries may have an obligation to retain the traffic data of all users for a specified time, so-called blanket traffic data retention. Other countries may provide only for data preservation where the ISP is ordered to preserve ('freeze') the traffic data of a specified user in respect of a specific criminal investigation.

The format of electronic information on the Internet is not always clear.[36] For example an unopened email waiting in the mailbox of an ISP until the addressee downloads it to her computer, may be considered either as electronic information in transit or in storage. If the unopened email is considered as electronic information in transit, interception will be applicable whereas if it is consider as information in storage, search and seizure will be applicable.[37]

---

basis. S 2 of this Act states that the interception takes place in South Africa and only if the interception is affected by conduct within South Africa. It is applicable to content data.

32 "Monitor" in terms of the Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002 is defined as "to listen to or record communications by means of a monitoring device." It is applicable to content data.

33 Traffic data retention is the retention of traffic data (not content) for a certain period of time of all users irrespective of whether the user is a suspect of a crime committed. There does not exist a uniform definition of traffic data.

34 Data preservation is the retention of the traffic data of a specific suspect for a period of time in respect of certain criminal investigation.

35 Decryption is used to access encrypted data.

36 Berkowitz Robert in "Packet Sniffers and Privacy: why the No-Suspicion-Required Standard in the USA Patriot Act is Unconstitutional" 2002 *Computer Law Review and Technology Journal* 3.

37 Nieman Search and Seizure, Production and Preservation of Electronic Evidence (2006 thesis North West University) states on 52 that some legal systems consider it as information in storage by someone other than the ISP and it can be obtained only by the power of search and seizure.

5. Convention on Cybercrime[38]

The Convention of Cybercrime (Convention) is a multilateral instrument aimed specifically at addressing crimes committed in an electronic medium (computing environment) such as the Internet. The aim of the Convention on Cybercrime is to combat cybercrime by requiring signatory countries to establish certain substantive offenses and adopt domestic procedural laws to investigate cybercrime, furthermore addressing criminal and procedural law on an international level to ensure the harmonization of laws governing the criminal justice systems and to provide international co-operation and assistance in criminal investigations.

Relevant in respect of surveillance, is section 2 article 14 – 21 of the Convention. The Convention provides for data preservation of specified traffic data for a maximum period of 90 days. It does not provide for compulsory traffic data retention. The Convention was signed about 2 months after 9/11 and it was not drafted against the background of terrorism. This may explain why the Convention provides for data preservation and not compulsory data retention. It also provides that a country have the ability to implement interception of data either with the assistance of service providers (indirect surveillance) or in circumstances where the service provider is not able to provide assistance, to be able to exercise the powers themselves (direct surveillance).

6. Brief notes on Internet surveillance laws

Although surveillance as an investigatory method existed prior to 9/11, 9/11 had a global impact and resulted in the extension and intensification of electronic surveillance and the implementation of surveillance laws by granting law enforcement and intelligence agencies with more surveillance powers.

The discussion of the surveillance laws of a specific country falls outside the scope of this discussion. However, when evaluating the surveillance law of a country, the following aspects should be taken into consideration:

a. The only international treaty on cybercrime, the Cybercrime Convention, serves as a yardstick to establish which countries were signatories to the Convention or have acceded to the Convention, whether the signatory country has ratified it and the extent to which a signatory country comply with the Cybercrime Convention.
   The surveillance laws of those countries that were not signatories or did not accede to the Cybercrime Convention, may be compared to the Cybercrime Convention to establish how their Internet surveillance laws differ from the Cybercrime Convention;
b. Although the Internet was not designed as a single entity with a single authority that governs the legal development and use of the Internet, dominant ‘powers’ have emerged in respect of the Internet legal regulation, such as the USA,

[38] The Convention was signed on 23 November 2002 by the Council of Europe member countries and four non-European countries, namely South Africa, Canada, USA and Japan. The USA ratified the Convention in September 2006 and it came in force in January 2007. Approximately 43 countries have signed the Convention.

European Union (EU) and China.[39] It is important to take note of the surveillance laws of the US and the EU and the extent of the influence of the dominant powers on the surveillance laws of other countries; and

c. Countries can also learn from each other by taking note of the deficiencies in and/or criticism leveled against a country's surveillance laws and try to prevent following suit, for example, some shortcomings have been identified in the surveillance laws of the US and criticism has been leveled against the EU Directive providing for data retention.

7. Some considerations regarding surveillance as an investigatory method on the Internet

7.1 The question is how can cybercrime be prevented, detected, investigated and a suspect be prosecuted?
Conduct regulation does not assist in the gathering of information on the Internet. To be able to investigate crime and prevent the Internet from becoming a 'lawless frontier', the investigator needs to gather information. Information gathering on the Internet can only be done by means of surveillance. After 9/11 most countries apply surveillance to the Internet;

7.2 Investigating a crime needs a harmonized global approach to assist in across border investigations. Although the global Internet community does not speak with one voice in respect of information gathering, there should be some consensus amongst the Internet community on the surveillance methods used to gather information;

7.3 Surveillance is made possible by means of technology that is increasingly becoming more refined and sophisticated. Surveillance may be non-obvious, but it is intrusive. Surveillance technology must be regulated, otherwise it can be abused;

7.4 Surveillance of information can violate human rights such as the right to privacy and the right to freedom of expression. Although surveillance legislation is imposed from the law enforcement side of government, it does not automatically justify the use of surveillance. Surveillance legislation must be scrutinized as it may infringe the rights of Internet users. It is important that surveillance laws provide for judicial oversight and compliance with prerequisites to prevent governmental abuse of surveillance as an investigatory method;

7.5 Surveillance is not only used for investigating a crime, but it may be seen as a security measure in protecting users' information against crime; and

7.6 EU countries are in the process of implementing traffic data retention legislation. Other non-EU member countries will most probably follow the EU's approach and implement blanket traffic data retention. In the US there is growing interest and pressure to apply traffic data retention to investigate, for example child pornography. Data retention has evoked a lot of discussion and it is relevant to take note of advantages and disadvantages of data retention.[40]

---

[39] Goldsmith and Wu *Who control the Internet* (2006) viii.

[40] See Watney "State Surveillance of the Internet: human rights infringement or e-security mechanism?" 2007 *International Journal of Electronic Security and Digital Forensics* 42 – 54.

8. Conclusion

The problem governments wish to address is the challenges inherent in the prevention, detection, investigation and prosecution of crime, terrorism and information warfare to ensure that the benefits of the Internet are maximized.

Goldsmith and Wu[41] says: "The greatest danger for the future of the Internet come not when governments overreact, but when they don't react at all." All stakeholders will agree that action on governmental level is required to ensure the growth and prosperity of the Internet but how far can government action pursue criminal justice before it amounts to an abuse of powers?

Many governments of Internet-connected countries have elected surveillance of information on the Internet as a solution to address the problem of cybercrime and terrorism. The question is whether the benefits of surveillance are in balance with the possible disadvantages, e.g. privacy infringement and possible abuse of investigatory powers. At present, most governments are of the opinion that the use of surveillance as an investigatory method is justified.

---

41 *Who control the Internet* (2006) 145.