

Annual ADFSL Conference on Digital Forensics, Security and Law


2007
Proceedings

The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism

Murdoch Watney

University of Johannesburg, South Africa, mwatney@uj.ac.za

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Watney, Murdoch, "The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 1. <https://commons.erau.edu/adfsl/2007/session-5/1>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism

Murdoch Watney
University of Johannesburg
South Africa
mwatney@uj.ac.za

ABSTRACT

Internet regulation has evolved from self-regulation to the criminalization of conduct to state control of information available, accessed and submitted. Criticism has been leveled at the different forms of state control and the methods employed to enforce state control. After the terrorist attack on the USA on 11 September 2001, governments justify Internet state control as a law enforcement and national security tool against the abuse and misuse of the Internet for the commission of serious crimes, such as phishing, child pornography; terrorism and copyright infringement. Some Internet users and civil rights groups perceive state control as an abomination which results in an unjustifiable infringement of civil rights. Since countries worldwide are focusing attention on the control of information on the Internet, the debate in respect of state control and the consequences of state control is relevant on a global level as it impacts on all Internet-connected countries.

Keywords: legal regulation, legal evolution, Internet, Internet state control, crime, terrorism

1. INTRODUCTION

The evolution of legal regulation of the Internet can only be fully appreciated by looking at the early beginnings of the Internet. The history of the origin of the Internet is well-known. However, to paraphrase Oliver Wendell Holmes, one must study the history in order to understand the path of the law (Rustad et al. 2002).

The Internet originates from the early 1960's in the United States of America (USA) as a result of a project referred to as ARPANET. This project aimed to ensure a nation-wide computer network that would continue to function even if a large portion of it were destroyed by a nuclear attack (Hiller et al. 2002).

In 1992 the USA congress decided to commercialize the Internet. Little did the USA realize that this historical decision would result in the information age characterized by a phenomenal growth of Internet-connected countries, contribute to globalization and the introduction of a new medium, namely an electronic medium.

The Internet's pace of adoption eclipses all other previous technologies. Radio was in existence thirty-eighty years before fifty million people tuned in; television took thirteen years to reach that benchmark. Fifty million people were using desktop computers only sixteen years after the first personal computer kit came out. Once opened to the general public, the Internet surpassed the fifty million mark in just four years (Rustad et al. 2002).

It was only in 1995 that the World Wide Web (WWW) became an integral part of the USA society, but today countries across the globe are dependent on the Internet. In the early days of the commercialization of the Internet and the growth of Internet connected countries, attention primarily focused on the development and use of information and communication technology. Initially scant regard was given to the legal regulation of conduct on the Internet.

As the dependence on computers, computer systems and the Internet increased issues such as copyright infringement and the threat and commission of crimes such as child pornography and 'identity theft' necessitated the implementation of legislation dealing with these issues. The attention

from the early days shifted from self-regulation to legal regulation of conduct on the Internet.

The terrorist attack on 11 September 2001, generally referred to as 9/11, was a watershed occurrence regarding state control of information available, accessed and submitted on the Internet. Attention focused on the form of state control of information and the methods employed to enforce state control of information. Although the USA was the first country to focus on these aspects, the global nature of the Internet, crime, terrorism and information warfare, render Internet state control relevant on a global level.

The world today looks very different from what it looked in 1992 when the Internet was commercialized. Governments now realize the power of the Internet. Some governments even fear the Internet.

Although no central legal authority governs the Internet, powers have emerged that influence the global legal regulation of the use and development of technology. The Internet laws of these powers affect the national laws of other Internet-connected countries (par. 3 hereafter).

It is important that the evolution of legal regulation is scrutinized and debated. State control can be likened to that of a Pandora's box. Once opened, it reveals many relevant issues that should be critically investigated. The forms of state control of information and the methods employed to enforce state control of information have serious consequences in respect of human rights and the role of third party's such as the ISP. Is this the type of Internet society we wish to live in or is the evolution of Internet legal regulation the prize we pay for security against crime and terrorism on the Internet? Should governments and the Internet user fear the Internet? How do governments and the Internet community determine the acceptable form for and methods of state control of information? Who will act as a watchdog in respect of the form of state control and the methods employed to enforce state control? These questions affect all Internet-connected countries and should be addressed within a global context.

The evolution of the legal regulation of the Internet is a very wide and complex topic with many inter-related issues of which each issue could warrant a discussion of its own. Therefore, the discussion will only be an overview of the most relevant issues from the perspective of a South African trained jurist.

2. OVERVIEW OF THE EVOLUTION OF INTERNET LEGAL REGULATION

Are the evolution of laws that regulate terrorism and crime on the Internet known and understood?

“...This is the Law. How could there be a mistake in that?”

‘I don't know this Law’, said K.

‘All the worse for you’, replied the warder” (Gringras 2003).

Initially the role of the law was perceived as irrelevant in respect of the Internet. It was felt that as the Internet was created by technology, it should therefore be regulated by technology.

Prior to the commercialization of the Internet in the USA, the close-knit Internet community regulated the Internet themselves (Harvard Law Review 2006). It was with some surprise and dismay when a member of this early community released the first worm, the so-called Morris worm (named after its creator) in 1988 (Rustad et al. 2002). The accused was successfully prosecuted in terms of the Computer Fraud and Abuse Act of 1986. However, when the ‘I love you virus’ was released in 2000, the global economic loss was substantial. The perpetrator was traced to Philippines but the conduct was not criminalized in the Philippines at that stage (Hiller et al. 2002). Subsequently the Philippines passed the E-Commerce Act.

The Internet was not founded on a secure foundation. It was designed to be open with distributed control and trust among each other (Harvard Law Review 2006). As Internet usage increased, the exploitation of the Internet by means of online crimes increased. The Internet had not been designed to cope with that type of security challenges. Security technology proved fallible. Countries realized that

due to the fallibility of security technology, the enforcement and violation of technology should be regulated by means of legislation.

Cybercrime proved different from crimes committed in a physical medium. The electronic medium challenges the laws designed for a physical medium. In many instances the physical laws cannot be extended to address the electronic medium. Online crimes are not contained within the national borders of a country. Countries therefore moved from self-regulation to legal regulation of conduct on the Internet by criminalizing certain forms of conduct.

A good example of the consequences of inadequate legal regulation of conduct on the Internet would be the legal position in South Africa from 1993 to 2002. When the Internet became commercial in South Africa in 1993, very little attention was given to the Internet due to the fact that South Africa was involved in a political transformation. The Internet became part of society without much fanfare. South Africa was also urged not to regulate the use and access to the Internet and warned that “excessive regulation or control of the Internet would backfire”, that “the Internet and its technology would render the controls worthless” and that regulation should be conducted “not with fear and prejudice” (Opperman 2000). However, the criminal abuse of the Internet created legal uncertainty as the criminal and procedural laws designed for a physical medium were not flexible enough to address the commission of crimes by means of the Internet. It was only in 2002 that South Africa criminalized conduct in cyberspace by means of the Electronic Communications and Transactions Act 25 of 2002, the first legislation that deals exclusively with the electronic medium.

Although there had initially been opposition to the legal regulation of the Internet, it would be a mistake to believe that the Internet was ever free of any form of regulation. Lessig in his book, *Code and other laws of Cyberspace* observes that absolute freedom does not exist in cyberspace as cyberspace is built on codes in the format of programming code such as software, hardware and protocols (Lyon 2003, Edwards and Howells 2003). Lessig suggests that technology should address problems experienced on the Internet, for example copyright infringement can be addressed by means of anti-copying technology in the format of digital rights management. Lessig also confirms that the regulation of code (technology) is being sanctioned and enforced by means of legislation (Bowrey 2005).

Until 9/11 countries were mainly concerned with regulating conduct on the Internet such as crime by means of legislation. Countries did not actively seek control of information available and transmitted on the Internet. 9/11 was a globalizing event that changed the westernized world in particular and evolutionalized the legal regulation of the Internet. The emphasis in this paper is on the motivation for, the justifiability, consequences and enforcement of legal regulation of Internet state control of information.

3. CENTRAL LEGAL ‘GOVERNANCE’ (REGULATION) OF THE INTERNET

Governance of the Internet, specifically legal governance, is very relevant to the discussion of the evolution of legal regulation of the Internet. 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 western ‘powers’ have emerged in respect of the legal ‘governance’ of the Internet, such as the USA and European Union (EU). Data protection (information privacy protection) and now data retention illustrate the role and influence of the dominant ‘powers’. It is important to briefly look at data protection as it is affected by state control and specifically, the method of data retention.

While the Internet serves as a tremendous resource for information, products, and services, the same technology provides companies and individuals the ability to collect information about Internet users and to distribute that information to others. Many Internet users feel that this collection of data is an illegal invasion of privacy, specifically information privacy which is defined as the right of an individual to control the acquisition, disclosure and use of personal information.

The EU responded by recognizing and protecting an individual's right to information privacy by implementing 2 data protection directives, namely the general data protection directive, 1995/46/EC and the specific privacy and electronic communications directive, 2002/58/EC. In terms of these data protection directives personal information may not be processed without the permission of the Internet user. 'Personal information' is defined as information that identify the Internet user whereas 'processing' is defined as the storage, collection, retrieval, use, blocking and disclosure of personal information.

Contrary to the USA that has favoured self-regulation in respect of the processing of personal information, most countries worldwide follow the example of the EU. However, criticism is leveled against self-regulation in respect of personal information in the USA. Momentum for legislation in the USA that requires protection of personal information and restricting the type of personal information that can be collected is accelerating (Schulz 2005).

In 2001 the only international treaty on cybercrime, the Council of Europe Cybercrime Convention was signed by the Council of Europe member countries and 4 non-European countries, namely the USA, SA, Japan and Canada. The purpose of this international treaty is to provide guidelines regarding harmonized laws to address prosecution of cybercriminals across border crimes. It was not drafted against the threat of terrorism. The Convention was signed about 2 months after 9/11. It is commendable that countries realized that online crime can only be effectively and successfully be addressed by means of harmonized laws with mutual international assistance. Even if users in the USA take effective security measures, computers abroad could still be used in an attack on a USA target (Harvard Law Review 2006). However, the Convention on Cybercrime only provides for international cooperation in prosecuting cybercrime but makes no provision in securing networks (Harvard Law Review 2006).

In respect of state control of information on the Internet, the USA was the first country to take the lead in respect of surveillance. Shortly after 9/11, the USA implemented Internet state control legislation providing specifically for surveillance. Alan Dupont, director of the Asia-Pacific Security Program in Australia, said, "Where the U.S. goes, others will follow" (Lyon 2003). It is therefore worth while to examine closely what is happening in the USA and to establish to what extent and degree it is followed elsewhere.

As illustrated the effect of global Internet 'governance' cannot be discounted. Countries outside these 'powers', such as Australia, South Africa and India model their national laws on the laws of the dominant 'powers' and international treaties to ensure harmonized laws. This has been the case with data protection and will most probably be the case in respect of the form and methods employed for state control of information on the Internet.

The global nature of the Internet necessitate countries such as the USA to take note of the concerns of other Internet-connected countries in respect of the Internet, such as technical 'governance' of the Internet and specifically the objection against the technical root being managed by the California based Internet Corporation for Assigned Names and Numbers (ICANN) under license from the US Department of Commerce (Bowrey 2006). Other concerns evolve around online security, cybercrime and censorship ("United Nations forum on control of the Internet opens in Athens" 2006). The latter concerns are all linked to state control of information on the Internet (par. 4 hereafter).

4. LEGAL REGULATION OF STATE CONTROL OF INFORMATION ON THE INTERNET

4.1 Introduction

The initial purpose of the Internet was to establish an open information and communication medium with easy and unlimited global access to any information free from any restrictions. Abuse and exploitation of the Internet resulted in the criminalization of conduct on the Internet. Criminalization do not address the challenges experienced in respect of the prevention, detection, investigation and

prosecution of cyber-crime, terrorism (Janczewski and Colarik 2005) and information warfare (Janczewski and Colarik 2005). It became increasingly clear that the key in fighting crime and terrorism on the Internet lie in the gathering of information. Governments started to investigate methods aimed at the control of information available, accessed and transmitted on the Internet.

9/11 was furthermore such a world event that immediately after 9/11 the United Nations (UN) Security Council passed resolution 1377 making it compulsory for all UN member countries to implement anti-terrorism legislation. Shortly after 9/11 the US passed the US Patriot Act providing for enhanced state control of information on the Internet in the form of surveillance. Although terrorism motivated the implementation of Internet state control legislation in the USA, it is also applicable to serious crimes such as organized crime and money laundering.

4.2 Forms of Internet state control of information

State control of information on the Internet can take on different forms. It consists of

- i. no access to the Internet as practiced by Cuba; or
- ii. censorship as practiced by China, Iran (“Iran bans fast internet to cut West’s influence” 2006) and Saudi Arabia; or
- iii. surveillance as practiced by USA, EU member countries and SA.

It is important that a distinction is drawn between surveillance and censorship. It should be noted that not only the form of state control, but also the methods employed to enforce state control that are relevant.

Surveillance is an umbrella term that means in its broadest to ‘watch over’. Surveillance of the Internet consists of various surveillance methods, such as monitoring, interception, encryption and data retention or data preservation.

Table 1: Surveillance methods

Surveillance method	Possible definition of such method
Monitoring	The listening to and/or reading of the content of a communication.
Interception	The acquisition of the content of a communication by someone other than the sender or recipient or intended recipient during the course of the transmission and includes monitoring as well as the examination, viewing and inspection of the content of the message.
Data retention Data preservation	The retention of traffic data of all Internet users irrespective of whether the Internet users are suspect or not in respect of terrorism or crime. Data preservation is the preservation of specific traffic data of an identifiable Internet user for a specific criminal investigation for a limited period of time. ‘Traffic data’ refers to data indicating the origin, destination, duration, termination, duration and size of the communication (Goemans and Dumortier 2003). Differently put it refers to the records kept by the ISPS when a user engages in online activity (Edwards and Howells 2003).
Decryption	Assistance in the decryption of an encrypted message.

The biggest debate at present is in respect of data retention as opposed to data preservation. On 14 December 2005 the European Parliament accepted a directive making it compulsory for all EU member countries to implement national legislation providing for the retention of all traffic data of all Internet users for a period of time. The Directive proposed a retention period of 6 months to 24 months. The EU directive does not prescribe the types of crimes that would be subjected to data retention but leaves it up to each EU member country to determine the categories of crimes subjected to data retention. EU member countries have until August 2007 to comply with the blanket data retention directive.

The Convention of Cybercrime provides for data preservation (discussed at par 3). The EU has deviated from the Convention. The main reason would be the threat of terrorism. Since the Convention on Cybercrime has been signed, there has been other terrorist attacks namely in Spain in 2004 and in the UK in 2005. Terrorism has been described as the threat of the 21st century. Data retention is not only aimed at terrorism, but also at addressing the commission of serious crimes. Contrary to the EU, the USA employs data preservation. However, even in the USA attention has focused on possible data retention, especially in respect of child pornography. The US Congress has said that federal legislation is needed to aid law enforcement investigations into child pornography (McCullagh 2006). The interest in the USA in respect of the EU's decision to retain all traffic data illustrates the far-reaching effect the EU's legal governance has in respect of the drafting and implementation of national laws in other countries (Morphy 2006).

South Africa (SA) has implemented the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2005 in September 2005. The act provides for data retention for a period of 3 years and is similar to that of the EU mandatory data retention directive.

It can be safely predicted that other Western countries will most probably follow the EU's approach in respect of data retention.

Contrary to state surveillance, state censorship is an ultra form of state regulation of control of information on the Internet. It includes surveillance but it goes even further; it limits and restricts access to all information and the free flow of information.

4.3 Effect of state control of information

Internet state control affects not only the Internet user but also the traditional role of the Internet Service Provider's (ISPs) as a conduit of information as well as strengthening and enhancing the powers of law enforcement and security agencies (see par. 5 hereafter).

State control results in a surveillance society and evokes a fear of a so-called Orwellian society with 'big brother' (the state) watching over the personal lives of everyone (Lyon 2003). One of the biggest concerns is that state control of information on the Internet is in conflict with an Internet user's human rights such as the right to privacy.

Privacy is not an abstract concept (McCellan 1976). The classic definition for privacy is the right to be left alone, but the definition has been extended to include the right to be free from unreasonable personal intrusion, or the individual's right to determine what personal information can be communicated and to whom (McCellan 1976). Privacy manifests itself as the power to control information (Defilippis 2006). Most western countries worldwide protect privacy, although the approach to privacy protection differs (Hiller and Cohen 2002).

Privacy has meaning only in relation to a national culture, a particular political system and a specific period of time (McCellan 1976). Privacy therefore, must be defined within the context of the Internet against the background of the threat of terrorism and government control.

Internet privacy consists of information (data) privacy and communications privacy. Information privacy means the control of an Internet user in respect of who has access to his/her personal

information, when and how. Communications privacy means protection against interference and/or intrusion regarding his/her communications, such as websites visited, e-mails sent and received, and use of search terms.

It is acknowledged that the right to privacy in an electronic medium such as the Internet faces challenges unknown to that of the physical world. There are virtually no online activities or services that guarantee absolute privacy ("Privacy in Cyberspace" 2006). ISPs and websites can monitor online activities, for example the ISP can determine which search engine terms the user used, which websites visited, the dates, times and durations of online activity. Furthermore, ISPs, websites and companies can collect personal information of the Internet user. The latter concern was addressed in the EU by means of data protection directives.

The Internet user can ensure privacy by means of privacy-enhancing tools such as encryption, using anonymous re-mailers; without the use of such privacy-enhancing technology, the Internet user has very little privacy regarding his/her activity on the Internet. As the Internet was not designed with security as its priority, these tools can also secure the communications. However, it should be borne in mind that these tools can also be used to hide criminal activity.

Contrary to surveillance that does not affect free flow of information, censorship not only affects the right to privacy but also the right to freedom of speech. Freedom of expression is the freedom of communication covering the full freedom to express ideas and information to send, circulate and to receive them (Goemans and Dumortier 2003). Furthermore, censorship has resulted in many controversial issues, such as whether a search engine should filter its search terms to comply with the government's censorship guidelines; whether a search engine should disclose to a government a dissident's identity; whether a search engine outside such a government should have business dealings with a government that support censorship? (Flint 2006). All these issues must be debated taking into account that the Internet community today represents a diverse cultural community with different viewpoints and agreement may not be easily obtained.

4.4 Justifiability of legal regulation of Internet state control of information

At what price do we secure the Internet? Clearly, a prize exists if we allow criminals unrestricted and unaccountable use of the Internet. At some threshold citizens expect their government to protect them against the crimes and terrorism committed by means of the Internet. It is therefore not only state control of information but also the threat of online crime and terrorism that affects the Internet user's human rights such as the right to privacy.

The risk of online crime and especially a serious online attack by terrorists or a foreign government is greater than ever; an online attack coordinated with physical attacks could compound the fallout by disrupting communications, distracting the government response and exacerbating the psychological damage from terrorism (Harvard Law Review 2006). Crimes such as 'identity theft' have grown exponentially over the past years. Criminalizing conduct on the Internet assists in the prosecution of an online crime and terrorism which is important not only to law enforcement but also to global security.

The challenge today lies in the prevention and investigation of online crime and terrorism. The law enforcement agency or national security agency needs evidence and this evidence (data) can only be found within an electronic medium. The traditional law enforcement tools cannot effectively address online crime (Harvard Law Review 2006). The traditional approach to crime has been reactive policing, namely the crime is investigated after it is committed.

As the threat of terrorism and seriousness of crime increased, attention was given to a different approach to the gathering of evidence than what was traditionally applicable within the physical world. Pro-active policing is the gathering of evidence before a crime is committed and assists in the prevention, detection, investigation and prosecution of crime.

The response to the security threats posed by terrorism and crime resulted in state control of the

Internet. The purpose of state surveillance as employed by the USA, EU member countries and SA is to gather information in respect of the detection, prevention, investigation and prosecution of crimes or intelligence gathering. It is aimed at national security and/or crime prevention. The surveillance method, data retention is an example of pro-active policing. The traffic data of all Internet users are retained for a period of time, irrespective of whether the Internet user is suspected of committing a crime.

State surveillance could therefore be seen as an e-security technological tool. As is the case with privacy, security does not have an exact meaning (Hiller et al. 2002). Security must be defined within the context it is applied. Security within the context of this discussion is the technology employed to protect information and/or networks against abuse such as the commission of serious crimes and terrorism. The technology employed affect information (data) and communications privacy. The degree and extent of the impact on Internet privacy depends on the type of technology employed and the purpose of the technology.

The aim of regulating the use of state surveillance technology is to ensure judicial checks and balances in respect of the use of such invasive, non-obtrusive but extensive technology in respect of Internet users. If surveillance technology is applied without legal regulation, it can easily be abused. However, the legal regulation of state surveillance does not make it automatically justifiable.

The justifiability of state control of information can only be established by weighing the purpose for state control against the infringement of human rights such as the right to privacy. The debate in respect of the various surveillance methods is one that has not reached its pinnacle yet. It has to be established whether the legal framework provides an adequate balance to the conflicting interest. Some argue that the privacy infringement is so extensive that it cannot be justified. Others argue that the purpose for state surveillance justifies the human right infringement. The aim of state surveillance is to protect the Internet user and the state against serious crime and terrorism resulting in the growth of trust and confidence in the Internet.

Whether censorship is justifiable would depend on the purpose of censorship weighed against the infringement of the right to privacy and freedom of expression. It should be borne in mind that censorship in respect of specific information for example child pornography available on the Internet or the prohibition of hate speech is not the same as censorship in respect of all information.

5. OVERVIEW OF ENFORCEABILITY OF LEGAL REGULATION OF THE INTERNET

Relevant to the evolution from criminalizing conduct to surveillance of the Internet is the practical enforceability of such legal regulation within an electronic medium. If not enforceable, then the legal regulation results in paper law. The issue of enforceability could warrant a discussion on its own and therefore only the consequence of the enforcement of state control will be highlighted.

Regulating the Internet is not easy. In the physical medium enforceability normally do not depend on the assistance of third parties. In respect of the Internet, ISPs administer parts of the networks within the borders of a country within the legal framework of that country. A country must therefore implement legislation that provides for ISP assistance in respect of the control of information. The role of the ISP emphasizes the major shift from regulating conduct on the Internet or differently put, criminalizing certain conduct on the Internet to control of the information. In respect of regulating control of information on the Internet the active involvement of the ISP, a third party is now crucial for the successful implementation of legislation.

The role of the ISP in respect of control of information and in this regard censorship regarding specific information was clearly illustrated in South Africa in respect of child pornography access and distribution on the Internet (Watney 2006). The South African legislator realized that although child pornography distribution constituted a crime in terms of the Films and Publications Act 65 of 1996, it was still being distributed and accessed in South Africa. The legislator amended the Films and

Publications Act providing the ISP with an obligation to monitor information to prevent access to child pornography. The problem is that the type of technology employed to monitor the information is not prescribed and filtering technology is not always successful in the prevention of all child pornography.

In respect of state control of information in the form of state surveillance, the ISP in South Africa must comply with the following obligations:

- a. have interception ability,
- b. have data storage ability; and
- c. assist law enforcement and intelligence agencies.

The evolution of legal regulation is reflected in the changing role of ISPs especially in respect of data retention. ISPs have objected to the retention of the traffic data of all users. ISPs have criticized the financial and practical burden in storing data, citing that the problem is not only retaining the data, but maintaining and securing the data warehouses (Goemans and Dumortier 2003). The effectiveness of retaining data in the prevention and detection of crime and terrorism has been questioned. It has been alleged that where the law enforcement agency or the intelligence agency requests traffic data, such request would generally be of an urgent nature but it may not be so easy for the ISP to quickly comply with the request. The counter argument is that law enforcement and security agencies need information to detect and prevent crime and terrorism. The ultimate purpose of the general retention of traffic data is to be able, in the case of a crime, to trace and to locate geographically and chronologically the end-user device that was used to transmit the initial information (Goemans and Dumortier 2003). Many crimes are committed across borders and therefore it is important that countries adhere to harmonized laws and in the case of the EU, harmonized data retention laws. What should be borne in mind is that the effectiveness of for example data retention can only be measured once all EU member countries have implemented data retention legislation.

6. CONCLUSION

The shift from criminalizing conduct to control of information is a major transition in the evolution of legal regulation of the Internet. The transition is only in its early phase.

State control of the Internet can be compared to that of the *djinn* of legend; once the genie is out of the bottle, its power is unleashed for both good and evil (Poore 2002). To quote Poore (2002):

Our interconnectivity through the Internet enables cost effective data transmission to almost any point on the planet. When the data facilitates lawful commerce or promote human rights the enchanting magic validates the technology. When the data facilitates murder and mayhem or governmental oppression, the baneful condemns the technology. A complete free society – if it is to survive – requires citizens who exercise self-restraint and who are willing to accept the consequences of failures of that self-restraint. At some threshold of failures, however, citizens demand of their government protection from each other. At some point, such protection curtails the freedom of citizens and the citizens find themselves in a police state. Thus the pendulum swings between anarchy and totalitarianism, between unbridled freedom and censorship, between anonymity (i.e. no accountability and Big Brother (i.e., no privacy). To achieve the balance of costs and benefits, we must first understand the problems we hope to solve.

The problem governments wish to solve is the prevention, detection, investigation and prosecution of crime, terrorism and information warfare to ensure the growth of the use of the Internet, the realization of the benefits of the Internet and stimulation of technological innovation. Many governments of Internet-connected countries have elected state control as a solution to the problem, thus the pendulum has swung from no Internet regulation to regulation of not only conduct but also information.

The phase of legal regulation of state control technology results in many unresolved questions that

should be addressed before state control regulation progresses. Once in motion, many other methods of control of information may follow such as the prohibition of encryption or anonymous communication. Do the use of state control technology and the legal regulation of it qualify as an e-security mechanism? If affirmative, can it be argued that the costs such as the erosion of Internet privacy is the prize we pay for the benefits such as Internet security? On a global level countries will have to debate the good and the evil of state control to ensure that the good of the evolution of legal regulation triumphs over the evil.

7. REFERENCES

Books

- Bowrey, K. (2005), *Law and Internet Cultures*, BPA Print Group, Australia, pages 20, 62 - 67.
- Gringras, C. (2003), *The Laws of the Internet*, Cromwell Press Limited, UK, page i.
- Hiller, J.S. and Cohen, R. (2002), *Internet Law and Policy*, Pearson Education Inc, New Jersey, pages 6, 7 – 76, 95, 98 – 102, 170 - 171.
- Janczewski, L and Colarik, A. (2005), *Managerial Guide for Handling Cyber-terrorism and Information Warfare*, Idea Group Publishing, USA, page 43.
- Lyon, D. (2003), *Surveillance after September 11*, Blackwell Publishing Inc, USA, pages 29, 158.
- Rustad, M. and Daftary, C. (2002), *E-business Legal Handbook*, Aspen Publishers, Inc, New York, pages xxxix, 5, 6.

Chapter in Books

- Edwards, L. and Howells G. (2003), “Anonymity, consumers and the Internet: where everyone knows you’re a dog”, in *Digital Anonymity and the Law: Tensions and Dimensions*, eds.C.Nicoll, J.E.J. Prins, M.J.M. van Dellen, TMC Asser Press, The Hague, pages 216 – 217, 222 – 224.
- Goemans, C. and Dumortier, J. (2003), “Enforcement issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-line Anonymity”, in *Digital Anonymity and the Law: Tensions and Dimensions*, eds.C.Nicoll, J.E.J. Prins, M.J.M. van Dellen, TMC Asser Press, The Hague, pages 165 – 172.
- McCellan, G.S. (1976), “Privacy in a Free Society,” in *The Right to Privacy*, eds G.S. McCellan, H.W.Wilson Company, New York, page 25.
- Opperman, C.P. (2000), “Internet Law in South Africa”, in *Cyberlaw@SA: The law of the Internet*, ed. R. Buys, Van Schaik Publishers, SA, page x11.
- Poore, R.S. (2002), “Computer forensics and privacy: At what price do we police the Internet” in *The Privacy Papers Managing Technology, Consumer, Employee, and Legislative Actions*, ed. R Herold, Auerbach Publications, New York, page 33.

Journal

- Author unknown (Editorial notes). (2006), “Immunizing the Internet”, *Harvard Law Review*, Vol 119, pages 2445 – 2463.
- Defilippis, A. J. (2006), “Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence”, *The Yale Law Journal*, Vol 115, pages 1086 – 1093.
- Flint, D. (2006), “Don’t be evil” *Business Law Review*, pages 102 – 104.
- Schulz, E. (2005), “Personal information comprises: It is time for the U.S. Government to wake up”, *Computers and Security*, Vol 24, pages 261 – 262.
- Watney, M.M. (2006), “Regulation of Internet Pornography in South Africa”, *Journal of Contemporary Roman Dutch Law*, pages 227 – 237, 381 – 395.

Websites

Author unknown. (2006), “United Nations forum on control of the Internet opens in Athens”
http://www.mg.co.za/printPage.aspx?area=/breaking_news/breaking_news_business/&a.
(30/10/2006).

Author unknown. (2006), “Privacy in Cyberspace”,
<http://www.privcy/rights.org/index,htm>, see file:E:\Privacy in Cyberspace.htm.

Author unknown. (2006), “Iran bans fast internet to cut West’s influence”
http://ww.mg.co.za/printPage.aspx?area=/breaking_news/breaking_news_international
(18/10/2006).

McCullough, D. (2006), “America debates data retention”
<http://insight.zdnet.co.uk/0,39020415,39263973,00.htm> (24/09/2006).

Morphy, E. (2006), “AG wants law compelling ISPs to hold Customer Data”
http://www.ecommercetimes.com/story/53142.html?u=crbuys&p=ENNSS_0be3a1d63b9517
(30/09/2006).

ABOUT THE AUTHOR

Murdoch Watney is a professor in the Faculty of Law at the University of Johannesburg, South Africa. She has worked as a prosecutor, is admitted as an advocate of the High Court of South Africa, has done the bar exam and has acted as an assessor in criminal trials in both the High Court and Regional Court. She has given papers at the following international conferences:

- 2005: Internet pornography: International Society for the Reform of the Criminal Justice System; Edinburgh, Scotland;
- 2006 “State surveillance of the Internet”: 2nd Annual International Conference on Global e-Security (ICGeS); University of East London, London, England
- 2006: “Surveillance of electronic communications: A consequence of globalisation?": ISSE (Independent European ICT security conference and Exhibition); Rome, Italy.

