THE UNIVERSITY OF CAPE TOWN

Faculty of Law – School for Advanced Legal Studies

NEW COMMUNICATION TECHNOLOGIES VERSUS NEXT GENERATION SURVEILLANCE LEGISLATION

PREVAILING TRENDS AND THEIR EFFECT ON THE PRIVACY OF COMMUNICATIONS

University of Cape Town

David Lunga

LNGDAV007

B.Bus Sci(Finance)

(Contact telephone number: +27 (0)82-0733-408)

Supervisor: Steve Ferguson

Cape Town

2011

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the degree of Master of Philosophy in Information Communication Technology Law, in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of Master of Philosophy dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

Declaration

I, David Lunga, hereby declare that the work on which this thesis is based is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree in this or any other university.

Signature: Signed by candidate

Date: 29/08/10

Table of Contents

LIST OF FIGURES AND TABLES

1. INTRODUCTION

The purpose of this paper is to explore the impact of new technologies on the nature, ambit and objectives of communications surveillance, particularly lawful access and interception. A particular focus on the privacy issues arising from new approaches has been examined by taking a close look at the sources of communications privacy rights and indeed expectations and the almost invariably antagonistic position of law enforcement in attempting to retain powers enjoyed under former lawful communications surveillance regimes.

Surveillance is taken in this paper as an umbrella term, encompassing the various techniques of investigation including interception of communications traffic or transactional data and the monitoring or recording of the content of communications.

A driver of the significance of these questions is the rise in use and pervasiveness of electronic communications reflected in three main effects[1]

1. Modern electronic communications have become too convenient and integral to business for most people to practically expect to avoid
2. The diversity of channels along which traditional written messages travelled has actually shrunk
3. The interception of electronic communications is likely invisible to the targets.

Communications surveillance from its earliest uses provided an important and powerful tool of investigation. This tool proved unprecedented in its ability to provide reliable information on criminal activities while reducing the risk to the lives of agents as well. Moles and informants could not provide the sort of information that could be garnered from surreptitious surveillance. The use of such techniques has not always been regulated however, with increasing use of interception coinciding with growing public awareness and disapproval of these methods as excessively invasive and as potentially infringing the privacy rights of citizens. Concerns over the government adopting a general spying regime in the same vein as Orwell's Oceania in the novel '1984' were vindicated as even

[1] Whitfield Diffie & Susan Landau *Privacy on the line: The politics of wiretapping and encryption: Updated and expanded edition* (2007) at 174.

societies considered free and open like the United States engaged in unlawful and gratuitous use of wiretaps to monitor the communications of those not suspected of any criminal links at all.

While not all jurisdictions have always recognised the validity of arguments for the privacy of communications, a substantial body of precedent in the common law has resulted in a de facto law of privacy, even in jurisdictions where constitutional rights make no express mention of privacy. Today communications surveillance is considered a staple of modern intelligence gathering and investigation. Law enforcement agents continue to rely on it to provide information on organised crime, and other serious offences such as international terrorism.

This paper will also explore the question of whether next generation surveillance laws have been used to expand the scope of investigatory powers granted to law enforcement, rather than to maintain previous minimum expected levels of investigatory power. International approaches to these problems have been investigated to provide a more informed view of the policy objectives of the South African interception regime as encapsulated in the Regulation of Interception Communications and Provision of Communication-related Information Act[2] (RICA)

Commentary outside of the jurisdiction specific chapters is kept relatively conceptual, owing to the widely differing treatments of terms like traffic data and even interception itself. This was with a view to keep the actual questions related to privacy and new surveillance measures separate from the review of the underlying legislation in each jurisdiction.

[2] Act 70 of 2002.

2. HISTORY AND SOURCES OF COMMUNICATIONS PRIVACY RIGHTS

2.1. Privacy rights versus the national and public interest

There is an inherent tension between the protection of privacy rights, and that of national security. Truly one of the most enduring moral and practical problems of communications surveillance and monitoring is the exclusion of non-target information and filtering for only the information being sought.[3] When communications are captured by human agents in control of recording or monitoring equipment, concerns regarding the potential abuse of the information gathered are also raised. In particular examination of information that is outside the scope of the warrant or not relevant to any the investigation.

Automated systems, depending on their level of complexity manage to allay some of the concerns of prying behaviour at the cost of potentially lower specificity where people other than the target might find their communications subject to recording or monitoring. Simpler automated systems might fail to exclude such communications, again introducing some form of subsequent filtering by humans, which would again raise the same concerns mentioned above.

National security encompasses aspects of repelling attacks by foreign military forces as well as domestic threats while not extending as far as to include all aspects of the national interest.[4] While the prevention of serious crime has always been included as an object of lawful surveillance legislation, the national interest has in fact been relied on to justify increasing the scope of communications surveillance to include a wider range of media and data types.

Protection of these national interests has also seen a greater insistence on secrecy requirements related to non-disclosure of details of surveillance performed by authorised persons. These changes can be seen to reflect recognition of the growing threat of international terrorism, and the complicated

---

[3] Diffie & Landau op cit note 1 at 95.
[4] Ibid at 87.

nature of investigating these activities, where the planning and coordination of attacks rely increasingly on electronic communications.

2.2. Privacy rights in the Council of Europe's Convention on Cybercrime

The Council of Europe's Cybercrime Convention of 2001(hereinafter 'the Convention') presented the first attempt at a formalised multilateral agreement on cybercrime. The Convention pursues the 'protection of society against cybercrime' ie criminal activities involving computer systems and devices, whether as tools or targets in these activities. Both the United States and the United Kingdom have signed and ratified the Convention, while South Africa though having signed, has yet to ratify it.

The objects of the Convention include the harmonisation of state laws on the prohibition and handling of cybercrime offences as well as the establishment of requirements for international cooperation in their investigation and prosecution. Aspects specifically dealing with approaches to interception and monitoring are contained in the Convention, as are some key provisions relating to the respect for privacy.[5]

Article 15 titled Conditions and safeguards in the 'implementation and application of the powers and procedures' requires that there be provision for

> 'the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality'

States are thus expected to promote the objects of the cybercrime convention while simultaneously upholding the commitments made in other multilateral agreements dealing with human rights, of which privacy of communications is a feature.

[5] The Council of Europe Convention on Cybercrime CETS No: 185, 2001 preamble.

2.3. The European Union Convention on Human Rights

Informed by the principles of the United Nation's Universal Declaration of Human Rights, the Council of Europe adopted the European Convention on Human Rights in 1950. The convention seeks to consolidate a common view of safeguards for human dignity and individual freedoms that had after World War II suffered serious setbacks, not least with the full consent of national governments.

Article 8 deals specifically with the expectations espoused in the Constitution of the United States as well as the United Kingdom's Bill of Rights relating to privacy and the associated rights of the individual:

> Right to respect for private and family life
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. 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.

These provisions while still subject actual interpretation and implementation in each jurisdiction, expressly intend to provide protection against arbitrary searches as well as protection for the correspondence individuals enter into. The freedoms are tempered by lawful and necessary "interests of national security, public safety, or economic well-being of the country" as well as in the prevention of crime and protection of the rights of others *inter alia*.

2.4. In US law

Privacy is not explicitly mentioned in the US Constitution, which initially complicated the view on the associated privacy of communications somewhat. Privacy rights in an American context thus derive from the common law, as courts have interpreted the Bill of Rights.

The Fourth Amendment deals with protections against unreasonable search and seizure, a protection that apart from the obvious physical search and

seizures prohibits the unauthorised monitoring, or listening in on an individual's communications.

The US Constitution: Fourth Amendment:

> 'The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

Collectively the protections afforded people by the Fifth, Fourth, Fourteenth, Third and First amendments provide a matrix that encapsulates our current understanding of the concept of 'privacy'.

2.5. In UK law

While the United Kingdom has no formal written Constitution, common law privacy principles reach as far back as the 17th century. Semayne's case established the requirement to knock before entering even when in possession of a warrant where "'[e]very man's house is his castle'"[6]

The Human Rights Act[7] stemming from the obligations under the European Council's Convention on Human Rights and Fundamental Freedoms forms the basis of statutory privacy provisions in the United Kingdom.

2.6. In South African law

Section 14 and 16 of the South African Constitution[8] provide for rights to privacy, and the privacy of communications in the protection of the privacy of correspondence. The South African position largely mirrors that of the United States with regards to privacy's extension to aspects of life where there is a

---

[6] Lusine Ajdaharian 'Knocking down the Knock-and-announce rule: A casenote on Hudson v. Michigan 29' (2007) *Whittier Law Review*.
[7] 1998 c. 42.
[8] 1996.

legitimate expectation of privacy, also qualified as that which society itself views as subjectively reasonable.[9]

2.7. Private data and privacy of communications

From privacy rights concerns stems the question of the proper treatment of private information. Generally this is information that is collected and stored, often with the permission of the person to whom that data relates. Typical examples would be the billing data necessary for a network operator to provide services to their customer, while billing them correctly. Different jurisdictions have adopted differing levels of regulatory oversight over these practices. Nevertheless there are certain principles that either in wording or substance feature in all the legislation adopted:

1. 'The keeper of any system of personal records is responsible for the safety, security and integrity of the data so stored.
2. The existence, purposes and workings of such systems should be readily accessible to public understanding.
3. A single figure (a 'privacy officer' or 'data controller') should be identified publicly as responsible for safeguarding the privacy interests affected by the working of each such system
4. Information held in such systems must be collected legally and fairly. Individuals must be able to review the content of information held on them in such systems and the uses and disclosures of such information; individuals must be able to obtain redress for inaccurate and inappropriate uses and disclosures of such data.
5. Personal data should only be collected in the form and to the extent necessary to fulfil the purposes of the system.
6. Personal data held in file should be as accurate and up-to-date as necessary to fulfil the purposes of the system.
7. Information collected for one purpose should not be used or released for other purposes, except under legal requirement or with permission of the individual.
8. Information held in file should be collected with the knowledge or consent of the person concerned.'[10]

---

[9] See Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC).

[10] James B. Rule *Privacy in Peril* 2ed (2007) at 26.

These principles are relatively comprehensive, however they focus on specifically on data that has been collected *and* stored. This data is often the sort that is retained in databases. While criminal investigations and issues of national interest involving the use of surveillance do tread the same lines drawn above, they are nevertheless not the essential focus of this paper. Points 6-8 describe the challenges that collectors of surveillance information face when trying to respect the privacy of for example, non-target communications.

Point 9 is particularly important in reference to real-time communications as it highlights the constant tension between legitimate privacy concerns of those subject to even lawful searches. The limitations placed on the ambit of a warrant of search for instance are not rights the target gains as such. Instead the warrant should be viewed as providing law enforcement with a means of legally infringing the rights of an individual under search.

In terms of legislation, protection of private information statutes have borrowed much from the Organisation for Economic Co-operation and Development (OECD)'s Guidelines on the Protection of Privacy[11] as well as the European Community's Privacy Directive of 1995.[12] Significantly what the Directive does is to set standards for member states, which are expected to codify the requirements into domestic law with provisions of equal or greater strength than those in the agreements.

The changes that came about as a result of the Directive very nearly led to a trans-Atlantic information Iron Curtain, where the precise requirements of the European legislation would have prevented export of data collected in Europe being sent to jurisdictions without similarly stringent data protection

---

[11] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Available at *http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html* [Accessed 20 December 2010].

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *http://www.cdt.org/privacy/eudirective/EU_Directive.html* [Accessed 20 December 2010].

requirements.[13] This would inevitably have led to a scenario contrary to that envisioned in the Cybercrime Convention which seeks to streamline and provide for easier data sharing and mutual assistance between investigative agencies across borders.

[13] William J. Long & Marc Pang Quek 'Personal data privacy protection in an age of globalization: the US-EU safe harbour compromise' 9 (2002) *Journal of European Public Policy.*

3. SOCIO-POLITICAL HISTORY OF COMMUNICATIONS SURVEILLANCE

3.1. Context

Indirect communications[14], being any form of communication not involving direct, face-to-face communications, have with time achieved two important ends that have been major drivers of their growth in use. These two ends are increased reliability of delivery and increased speed of delivery. Similarly, an associated drop in the cost of the use of indirect communications has seen not just a growth in use, but an undeniable reliance on the availability and integrity of these systems.

Indirect communications, the most rudimentary of which were letters sent via messengers. These letters and communiqués were at a relatively high risk of being opened and read, or 'intercepted' in the modern understanding of the concept. Depending on the level of skill and determinedness of the interceptor not to have their acts revealed to the recipient, these interceptions could remain completely secret from the sender and the intended recipient entirely. It was cognizance of this that pushed users of such delivery methods to rely rather on direct communications for matters of great sensitivity or import, relying on the 'encryption' afforded them, with secrets whispered quietly, out of earshot of all but the intended listener.[15] Rather than rely on the invocation of rights to privacy, those wishing to keep their matters to themselves chose either not to speak of them, or to pick their forums with care.

Over time however, technological changes have helped transform perspectives on indirect communications. A messenger robbed or taken ill along the way to deliver his charge was replaced by a wire and electric signals that with little delay informed one when one's words were not clear and not received, by the very person they were intended for. Therefore, with convenience grows a

[14] This is a term adopted in the South African lawful access legislation, the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).

[15] Diffie & Landau op cit note 1.

sense of trust in the systems used. Thus, increasingly sensitive and private content is sent via these media.

A broken seal upon an envelope betraying the interception of one's communication is replaced by a completely transparent and undetectable monitoring machine, capable of not merely relaying the gist of one's message, but an identical copy of it as well. Modern interception and monitoring possibilities by those authorized by legal powers and working outside of legality is invisible to the typical user, despite the flux of sensitive material disseminated across telephone networks, and internet communication services.[16]

Given this environment, few options are left to users who might wish to remain relatively certain of the privacy of their communications. Building their own networks and telephones is hardly practical, leaving a certain feeling that users must simply sit by and accept that Big Brother is listening and watching.

Complex legal questions are raised in this regard, given the fact that 'communications' have evolved substantially from being simple aural signals over a telephone. It is trite to point out that there has not ever been a universally accepted standard in terms of the privacy rights and the need for communications surveillance, even when the more simplistic plain old telephone system (POTS) network was prevalent.

3.1.1. History of communications surveillance in the United States

In the United States, the privacy of communications of individuals has long been viewed as a reasonable expectation, however in practice the requisite prohibitions on illicit use of communications surveillance have not long been enshrined in statute.

[16] Diffie & Landau op cit note 1.

The use of wiretapping by law enforcement agents was seen to arise virtually in tandem with the development of telegraphic communications[17] and telephonic communications.[18] The first significant attempt at regulating the use of wiretapping was the Anti-Wiretap Statute of 1918[19] that was actually an outward-facing piece of legislation, intended to prohibit the use of wiretaps by enemy forces within the US as opposed to controlling the use of wiretaps by domestic law enforcement agents.

It took almost a decade for the failure of Congress to regulate communications surveillance to be put before the courts to rectify. Roy Olmstead faced charges of running a bootlegging business, selling alcohol during Prohibition.[20] Key portions of evidence leading to his conviction were obtained from wiretaps that had been installed without a search warrant. Olmstead appealed the case up to the Supreme Court. The issue in question the manner in which the evidence used in his conviction was obtained.

The court acknowledged that the wiretaps were warrantless, but argued that to invoke Fourth Amendment protections against search and seizure, there necessarily needed to be a search, which in the courts view the wiretap did not amount to. The claim was 'There was no searching...The evidence was secured by the use of...hearing and that only...'.[21] The court's interpretation of the concept of a 'search' implied a physical or tangible element, which in the case of wiretaps and virtually all forms of surveillance is absent. The court, expected to uphold constitutional protections was caught napping, focusing on the form rather than the substance of the actions involved.

The minority opinion penned by Justice Brandeis emphatically illustrated the far-reaching insidious implications of the ruling:

---

[17] Sarah Boucher & Edward Cotler & Stephen Larson 'Internet wiretapping and carnivore' 2001 Available at *http://groups.csail.mit.edu/mac/classes/6.805/student-papers/spring01-papers/carnivore.doc* [Accessed 27 December 2010].

[18] Boucher & Cotler & Larson op cit note 17.

[19] 40 Stat. 1017 in Diffie & Landau op cit note 1 at 177.

[20] Diffie & Landau op cit at 178.

[21] *Olmstead v United States*, 277 US 438, 1928, p 464 in Diffie & Landau op cit note 1 at 177.

> 'Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.'[22]

The cost to the public was that their communications would remain unprotected least from wiretapping until the early 1930's with the passing of the Communications Act.[23]

While the Communications Act aimed to restrict the use of wiretaps by prohibiting the "interception and divulgence" of communications, aggressive moves by the director of the FBI J. Edgar Hoover to ensure continued use of wiretaps in limited circumstances in the interests of national security saw their continued use despite their lack of admissibility in court.[24] When evidence of Hoover's use of wiretapping came to light he set out to ensure that details of the use of wiretapping remained separate from that of the main case.[25]

The 1950s and 60s saw widespread abuse of the mandate granted to law enforcement with the meaning of 'subversive activities' being extended so as to include monitoring of suspected communist sympathisers, civil rights movement leaders as well as Supreme Court justices by the FBI.[26] It was only in the late 1960s that public opinion turned sharply against warrantless government interception of personal communications and the ease and gratuitous use of this technique came to the fore.[27]

---

[22] *Olmstead* supra note 21 at 475-6.
[23] 1934.
[24] Diffie & Landau op cit at 178-180.
[25] Ibid.
[26] Ibid at 179-185.
[27] Boucher & Cotler & Larson op cit note 17.

3.1.1.1. Katz v. The United States

Katz v. United States[28] provided the Supreme Court with a second chance to clean the dust off the Fourth Amendment rights against search and seizure that had effectively been set aside by the Olmstead decision.

Charles Katz was accused of making illegal bets using "an interstate communication facility" – that being the public telephone booth of a certain bank in Los Angeles.[29] Agents from the FBI had observed Katz's movements for some time and believed him to be involved in the illegal activity for which he was subsequently charged and convicted. These agents, attached monitoring devices to the outside of the telephone booth Katz was to use, and began recording as soon as he approached the booth.[30]

This case was taken up to the Supreme Court, having had the Court of Appeals for the Ninth Circuit uphold the initial judgment that found no violation of the Fourth Amendment in the use of surveillance of communications made in a public phone booth without a search warrant. The Supreme Court differed substantially finding that even a telephone booth would constitute an area where a person has a reasonable expectation of privacy, and that both electronic and physical intrusion into such a space would constitute a violation of the Fourth Amendment.[31]

This pivotal judgement, by excluding the materiality or physical nature requirement of an invasion of privacy effectively made warrantless interception of communications illegal. The dissenting view by Justice Black does have some implications for current policy on the issue. Justice Black held the view that the courts were not meant to play a reforming role but rather maintain one of solely being interpreters of the law. Black maintained that telephonic surveillance is similar to the act of eavesdropping. Eavesdropping itself being

---

[28] *Katz v. United States* 389 US 347 1967.

[29] Edmund W. Kitch 'The Limits of the Fourth Amendment' (1968) *The Supreme Court Review* 133 – 152. Available at *http://www.jstor.org/stable/3108771* [Accessed 15 June 2011].

[30] Ibid.

[31] Justice Stewart in *Katz v. United States.*

possible without technological aid would have been known and explicitly mentioned in the wording of the Fourth Amendment had the intention to extend the protections afforded therein to such situations been held. He thus maintained that the Supreme Court was in essence trying to shoehorn this interpretation into the Fourth Amendment.

If Justice Black's view is to be rejected as fundamentally flawed, then the role of the courts can be one of ensuring that interpretations of the law as written are coherent, and match the substance (the spirit in which the law was written). The courts' role then extends beyond mere semantics. In the context of electronic law, exercising this power can work to prevent laws from becoming obsolete or of no effect in keeping with the intentions of the original writers of the law. The onus to keep laws relevant retrospectively cannot fall solely on the legislature.

Title III of The Omnibus Crime Control and Safe Streets Act of 1968 can be seen as being the earliest example of lawful interception legislation that has been most formative in influencing the direction of current regimes. The act prohibits wiretapping in general, while providing the necessary exceptions for law enforcement agents to do so with the authority of a court order.[32]

The entire process of implementing a wiretap required first the submission of an affidavit showing that there was probable cause that the target communications were in the view of committing an offence. A government attorney subsequently prepares an application for a court order with the approval of a member of the Department of Justice. Finally at the expiration of the wiretap order the target is to be notified of the surveillance.[33]

---

[32] James Dempsey in Boucher & Cotler & Larson op cit note 17. Further, this was contingent on there being suspicion of serious crimes as well as proof that alternative investigative methods had shown to be needlessly ineffective or dangerous.

[33] It is worth noting that interceptions under FISA remain classified with only the reporting of the number of applications for orders as well as the actual directions granted being filed with the Administrative Office of the United States Courts.

3.1.2. History of communications surveillance in the United Kingdom

The United Kingdom quite unlike the United States has no written constitution, and thus privacy rights are instead enshrined in the common law and directives of the European Community.[34] Interception of telephone communications was until 1937 carried out without a warrant issued by the Secretary of State, while postal communications and letters had enjoyed this protection from as early as 1663.[35] The Guidelines of 1951 issued by the Home Office prescribed the requirements for authorization of a warrant by the Secretary of State:[36]

1. The offence must be serious
2. Normal investigative methods exhausted or proved to be likely to fail if attempted
3. A good expectation to believe the interception would result in a subsequent conviction

The conviction requirement was subsequently made less stringent[37] which gave effect to the protections provided for in the European Council Convention on Human Rights. One such protection being the determination that mechanisms to appeal what appears to be wrongful interception be provided for as a counterweight to frivolous or abusive use of interception by law enforcement agents. The United Kingdom would remain without legislation specifically dealing with interception regulation until 1985 with the Interception of Communication Act (IOCA).[38]

3.1.3. History of communications surveillance in South Africa

The South African approach to surveillance and interception began with interception of postal articles as well as telephonic communications through s

---

[34] Rule op cit note 10 at 64.
[35] The 'Interception of communications in the United Kingdom: A consultation paper' 1999 at 10.
[36] Ibid at 10.
[37] Ibid.
[38] Chapter 56 1985.

118A of the Post Office Act.[39] This amendment was inserted in recognition of matters relating to the security of the state.[40] These powers were initially overbroad and could be invoked by any government minister, which was reviewed and amended in the Interception and Monitoring Prohibition Act of 1992 to allow directives from "only a judge or designated retired judge of the Supreme Court".[41]

S v A[42] provided judicial precedent that has been upheld even after the establishment of constitutional protection of rights to privacy, where a private investigator installed a listening device into the plaintiff's apartment on orders from his estranged wife so as to acquire evidence of his alleged infidelity. The courts ruled this to be an unlawful invasion of the plaintiff's privacy, and the detective was found guilty of *crimen iniuria*[43] a common law delict. This requirement for authorization through a warrant was reiterated in S v Naidoo.[44] False information was given to the judge in the application to obtain an interception direction, which led to the direction itself being declared unlawful and the monitoring considered outside of the lawful limitations on the right to privacy.[45]

Nevertheless, the existing position seems to be that there must be an 'overriding justification of public interest' for certain interceptions that are unlawful to be considered reasonable limitations on the right to privacy. This needs to be assessed casuistically taking into account the underlying principles

---

[39] Act 44 of 1958 in Tracy Cohen 'But for the nicety of knocking and requesting a right of entry: Surveillance law and privacy rights in South Africa' (2001) 1 *The Southern African Journal of Information and Communication* available at *http://link.wits.ac.za/journal/j-01-tc.htm* [Accessed 2 January 2011].
[40] Ibid.
[41] Ibid.
[42] 1971 2 SA 293 (T).
[43] Ibid.
[44] 1998 1 BCLR 46 (D)
[45] Yvonne Burns *Communications Law* (2009) at 182.

intended in s 14 and 15 of the bill of rights balanced against the s 36 (1) limitation provision.[46]

[46] Cohen op cit note 39.

4. SURVEILLANCE – TOOLS, MECHANISMS AND STANDARDS

The Cybercrime Convention provides some conceptual insight into possible working interpretations of interception, and the legal perspective behind regulating it. While the scope of the Convention is aimed at "computer systems" specifically, the changing nature of communications in general towards being heavily dependent on digital exchanges and packet-switching technologies that necessarily involve some form of computing systems in the creation, transmission or retrieval of the communication.[47]

The Convention, as is typical of most multinational treaties leaves the enactment of complying laws to the signatories, while allowing ratifying parties to provide for standards that are at least as strict as those contained in the treaty itself. While issues such as precise definitions and treatments of what is considered interception and monitoring is left to the individual states, Articles 2 and 3 describe concepts of 'illegal access' and 'illegal interception' which have permeated most modern lawful access legislation.[48]

---

[47] As defined in Article 1 a) as '...any device or group of interconnected or related devices, one or more of which pursuant to a program, performs automatic processing of data;'.

[48] Key provisions aimed at limiting the possibility of 'over-criminalisation' include

i) Intentional actions where access or interception must be 'committed intentionally'

ii) An allowance for monitoring by say employers or universities who might incur liability from the use of their computing systems prohibiting access or interception only 'without right'. Similarly further protections could be provided through the potential requirement that access or interception be 'in relation to a computer system that is connected to another computer system'. This would provide say universities with sufficient right to monitor or intercept certain kinds of communications within their own network.

iii) Technical means which
'relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation', as described in the Explanatory Report para 53 available at *http://conventions.coe.int/Treaty/en/Reports/Html/185.htm* [Accessed 27 February 2011].

Signals intelligence is possibly the broadest overarching aspect of surveillance, where 'information [is] obtained by analysing signals emitted by a target. It is distinct from communications intelligence which describes attempts to actually extract information from a target's communications.[49] The distinction though subtle speaks volumes to the changes in lawful access and lawful interception regimes which have under the auspices of *maintaining* existing investigatory powers shifted further than justified into the realm of signals intelligence. The result is law enforcement is now able to glean a wider range of information such as locational data, and search habits than initially envisioned under older interception regimes.

4.1. Subscriber, Content vs. Traffic Data

There are effectively three broad classes of data types held by providers of communications services.[50]These are Customer Name and Address, and Local Service provider Identification (CAN/LSPID), Traffic data and Content data. Typically the level of protection for the data types increases with the sensitivity of it, with Customer Name and address as the least protected and content data enjoying the greatest level of protection.

4.2. Illustration of the different data types

Early interception prohibition regimes, when the predominant communications system was still the Plain Old Telephone System (POTS), made a distinction between the content of a conversation and the associated traffic data.[51] A simple example will serve to illustrate the different kinds of data and the significance of the difference in treatment. Tom phones his friend Jane, and reveals to her that he is suffering from terminal cancer. He confesses that he has told no-one else, not even his employer or wife. The traffic data associated with this conversation would be the telephone numbers of the parties (Tom and

---

[49] Diffie & Landau op cit note 1 93-4.

[50] Kerr and Gilbert in Dominic Cull *ISPs in the middle* (unpublished LLM thesis, University of Cape Town, 2004 at 2.

[51] Ian Hosein & Alberto Escudero-Pascual 'Questioning lawful access to traffic data' (2004) 47 *Association for Computer Machinery* 77-82.

Jane), the duration of as well as the date and time of the call. The content data would be the actual information conveyed, in the literal sense as the words spoken by the two parties, as well as the ideas related such as Tom's condition. The drafting of most lawful interception legislation has always been cognizant of a material and important distinction between the two kinds of data above. While the potential sensitivity of the conversation is no doubt a consideration, the letter of the law has effectively created a hierarchy where whether the conversation's content was related to what the parties of the call wished to have for lunch, or matters of deeper import as in the former example, the treatment would remain the same. A judicial warrant or a warrant authorised by the Secretary of State is needed to access the content data.[52]

The question of availability is another factor when looking at the justification for relatively easier access to traffic data. As an essential part of service provision, phone companies gain access to dialling information so as to route calls, and retain traffic data for billing purposes. In the United States this has reinforced the lower threshold required to access traffic data as it is data that the customer in fact shares with non-parties to the communication regularly for the purposes of executing the communication.[53]

4.3. Issues arising from new data types

While content data in the age of the POTS would have been obtained by wiretapping the conversation between Tom and Jane, in next generation networks sensitive information can be gleaned from data that might at first instance be classified as traffic data. The subject line in an email can contain what traditional methods would define as content data while being treated as traffic data owing to definitional ambiguity. The same can be said of the Uniform Resource Locators (URL) that users enter into their computing devices. Entering terminaldiseases.com could potentially reveal information more sensitive in nature than that given by traffic data in the POTS.

---

[52] Hosein & Escudero-Pascual op cit note 51.
[53] Ibid.

Remote Authentication Dial-In User Service (RADIUS) data from the remote access of users to the servers of internet service providers can be used to provide locational data of a specific user[54] As the user travels from one location of access to another, the authentication data remains the same, providing slightly more telling information than traffic data from a static location in POTS.[55]

Ultimately it is vital to be clear that technology neutral policy in terms of the provision of access to different data types can in fact be harmful. The sensitivity of content data and its requisite extra protection is a moot point; however analysis of traffic data can yield equally sensitive and potentially more telling information than purely communications data alone.[56] As Hosein and Pascual note, content data is generally only what the giver chooses to share and relate, while traffic data analysis can yield far more intimate knowledge of supposed or actual intentions, habits and beliefs.[57] Changes in lawful access provisions in terms of data types cannot be ignorant of these changes for the sake of technology neutrality.[58]

4.4. Preservation, Retention, Real-time

There are three 'collection and access methods'[59] typically referred to as Preservation, Retention and real-time data.

4.4.1. Preservation

This is the 'access to specified data or a specific user collected by service providers for business purposes'.[60] Also referred to as call logs in the case of

---

[54] Ibid at 80. The authentication details needed to log in to one of these servers necessarily proves that the user is who they say they are; whether that be an individual logging into their private account or using a company account. Practically this could be John Smith being logged in as *jsmith@.home.com* or *Jsmith@corporate.com* both giving at least *some* information on who is logging in at any given point.

[55] Ibid.

[56] Ibid at 82.

[57] Ibid.

[58] Earl of Northesk in the UK House of Lords regarding RIPA in Hosein & Escudero-Pasual. Op cit note 51 at 78.

[59] Hosein & Escudero-Pasual. Op cit note 51 at 81.

[60] Ibid at 82.

voice network operators this is typically the information related to the usage of whatever service is provided by the operator to the client with whatever characteristics necessary for accurate and timeous billing. Examples include duration of the call or service usage, whether the call was a regional or international call, any special rates or discounts applicable and other pertinent data.[61]

4.4.2. Retention

Retention is the 'requiring of all logs for all users be stored beyond their business purpose'.[62] Retention of data is a disputed practice as it places an additional financial burden on operators the benefits of which accrue solely to the users of retained data: law enforcement and government agents. Business processes and purposes will over time typically condense and anonymise data as retaining highly specific data on past transactions becomes less relevant and necessary with time. Preservation however demands that such processes not interfere with the data types required to be stored *and* kept 'secure and safe'[63] from 'loss or modification'[64].

From the point of view of businesses required to retain such data, this is a cost and administrative burden. Data retention rules are not a feature of US law at this stage, while the United Kingdom has established rules on it through the Anti-Terrorism, Crime and Security Act of 2001.

---

[61] There is some overlap to be expected in this and the data known as traffic data (or communications-related data) where the actual numbers dialled might be preserved as well for the purposes of monthly billing and in the case of resolving billing disputes with the client.
[62] Hosein & Escudero-Pasual. Op cit note 51 at 82.
[63] Council of Europe Explanatory Report op cit note 48 para. 151.
[64] Article 16 (1).

4.4.3. Real-time

Real time 'government access to real-time data flows' which allow for the collection or recording through technical means of traffic and content data in real-time as per lawfully authorised direction.[65]

[65] Article 20.

5. NETWORK TOPOLOGIES, DISRUPTIVE TECHNOLOGIES AND NGNS

Telecommunications operators fall into essentially two types of networks known as 'core networks' and 'access networks'.[66] The core networks are the high-capacity links that exist to connect sub-networks[67] often referred to as the backbone of a communications network. Access networks are what allow subscribers to actually access communications, such as PSTN, 3G and ADSL networks.[68]

5.1. The Public Switched Telephone Network (PSTN)

The Public Switched Telephone Network (PSTN) is a circuit-switched network[69] primarily used for voice communications and is the most common and simplest network for fixed-line voice communication provision globally.[70] The connection between two users in a voice call over PSTN uses circuit-switching, which effectively establishes an electrical link between the two devices.[71]

In purely analogue exchanges, voice calls on the network were entirely open to interception, with monitoring devices being positioned at any point from

---

[66] Philip Branch 'Lawful Interception of the Internet' (2003) 1 1 *Australian Journal of Emerging Technologies and Society* 38 at 39.

[67] Ibid.

[68] Ibid.

[69] A network where communication between two devices is contingent on establishing an electrical circuit between them. For more see the TCPIPGuide.com 'Circuit switching and packet switching networks' Available at *http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm* [Accessed 20 December 2010].

[70] IIT Kharagpur 'Module 1 Communications networks' Available at *http://nptel.iitm.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Communication%20network/pdf/1.1%20Lesson%201.pdf* [Accessed 8 August 2010] and Technologies for Conservation and Development 'Introduction to Communication Technology' Available at *http://www.t4cd.org/Projects/Current%20Projects/Documents/Training%20Manual%20-%20Communications%20Technologies.doc* [Accessed 27 December 2010].

[71] Technologies for Conservation and Development 'Introduction to Communication Technology' Available at *http://www.t4cd.org/Projects/Current%20Projects/Documents/Training%20Manual%20-%20Communications%20Technologies.doc* [Accessed 27 December 2010].

the actual telephone receiver, junction box, and telephone exchange frame.[72] Thus network topologies of this kind are inherently vulnerable to interception. Until the signal reaches the frame at the exchange where the lines are put into numerical order and then the call routed on to the receiving telephone, the path is unique to that specific telephone line.[73]

Having established a connection, that particular connection route or circuit is used exclusively to transmit the voice data, and kept open for the duration of the telephone call.[74] In a system such as this, law enforcement agents with a lawfully issued warrant have relative certainty that the communications they intercept are in fact those of the target's telephone alone.[75]

5.2. Shift to IP and Packet-switched networks

While early PSTN networks were geared primarily towards the transmission of voice, over time with the emergence of hybrid exchanges[76] which have become

---

[72] Diffie & Landau op cit note 1. Voice signals are received through the microphone of the handset, and then transmitted from the phone to a line cord and wall socket. The signal then travels to a phone closet, in the case of business premises with multiple phones, then on to the junction box and onto the most conspicuous part of most traditional telephone networks; the pole phone lines. From here it travels to another junction box, and then to the local telephone exchange where it is received on a frame.

[73] Diffie & Landau op cit note 1 at 131. The salient point is the dependence on a dedicated path (the circuit) per call in circuit-switched networks, as compared to one where packets travel along any number of changeable paths in travelling to their destination in packet-switched networks. For an illustration of circuit switched networks as compared to packet-switched networks. See also Figure 1. and 2. of the TCP/IP Guide. Available at *http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm*. [Accessed 20 December 2010].

[74] TCPIPGuide.com 'Circuit switching and packet switching networks' Available at *http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm* [Accessed 20 December 2010].

[75] Diffie & Landau op cit note 1 at 218. Absolute certainty is however not possible – In the United States, agents are required to turn off any recording device as the conversation being intercepted meanders to issues unrelated to the investigation. This requires an agent to be actively listening at all times that the recording device is in use- a significant factor in the overall cost of using wiretaps in the United States.

[76] Circuits where additional network services coexist, such as packet switching for access networks or VoIP gateways in interconnecting operators. See Montgomery, Patrick W 'A study into next generation networks for voice services: History, design and policy implications'

more common place, there has been convergence of media transmitted over the same channels.[77] Technological shifts have caused a shift towards packet switching networks, often referred to as Next-Generation Networks (NGNs), which are intelligent networks based on the Internet Protocol (IP).[78]

Part of the difficulty introduced by packet-switched infrastructures as compared to even digital circuit-switched networks is that unlike intercepting communications along a given circuit, and having the certainty that the conversation being monitored is that of the target(s) alone, packet-switched networks are host to streams of data that could include emails, voice, video and internet searches, that lack can lack the sort of identifiability and specificity inherent in the older topologies.[79]

From these changing topologies and mechanics arise legislative difficulties. Any legislation that makes it easier to listen-in on conversations is bound to generate a great-deal of opposition, lowering the likelihood of it passing into law. Thus lawmakers, under pressure from law enforcement to make *some* sort of change might attempt to skip this legislative hurdle by making amendments to the law rather than wholesale changes.

Other means of trying to regulate communications in the absence of specific legislation is to use the power to issue directions through underlying statute in order to expand the scope of rules, as done by the FCC in the United States, or the Home Office in the United Kingdom. This is problematic, as the mechanics of NGNs and packet-switched networks are inherently different and complex. There is no guarantee that an equilibrium where previous powers

---

available at *http://in3.dem.ist.utl.pt/master/thesis/03files/40thesis.pdf* [Accessed 20 December 2010].

[77] Sharon Black *Telecommunications law in the internet age* (2002) at 23.

[78] Patrick W Montgomery 'A study into next generation networks for voice services: History, design and policy implications' available at *http://in3.dem.ist.utl.pt/master/thesis/03files/40thasis.pdf* [23 December 2010].

[79] Ian Hosein 'The collision of regulatory convergence and divergence: updating policies of surveillance and information technology'(2002) 12 *The Southern African Journal of Information and Communication* 18 at 20.

given to law enforcement can be achieved while still preserving the same level of protection of privacy rights upheld thus far.

What is clear is that the problem of interception capability is one that needs to have been implemented prospectively, as it requires changes in the very architecture of the internet and the way it works, rather than a retrospective change now that the pieces are all in place.[80]

5.2.1. What is a protocol

A protocol is a set of rules governing how data is transferred and compressed over a network as well as its presentation on retrieval.[81] Common protocols include the hypertext transfer protocol (http), for transmitting and displaying web pages[82] and Voice over Internet Protocol (VoIP) which optimizes the transfer of packets over certain networks allowing while maintaining a quality of service that allows the outputs to be intelligible to a human user on either end.

5.2.2. What is a packet

A packet is comprised of control information, that being the source and destination address as well the actual piece of data requested itself whether that be a portion of an MP3 audio file, or a portion of a webpage.[83]The IP or Internet Protocol and packet technology are essential elements of modern communications networks, while also being the source of great difficulty in lawful access and lawful interception legislation.

5.3. Specialist networks and or communications protocols

5.3.1. VoIP

While VoIP is lauded for its versatility and robustness through its IP based transmission of voice data this flexibility is a double-edged sword for interception

---

[80] Susan Landau 'Security, wiretapping and the Internet' (2005) 3 *IEEE Security and Privacy* 31.
[81] Nadeem Unuth 'What is a protocol' available at *http://voip.about.com/od/voipbasics/g/protocoldef.htm* [Accessed 26 May 2011].
[82] Unuth op cit note 81.
[83] Fa-Chang Cheng & Wen-Hsing Lai 'An overview of VoIP and p2p copyright and lawful interception issues in the United States and Taiwan' (2010) 7 *Digital Investigation* at 82.

efforts owing to the connectionless nature of packet data flows as compared to traditional circuit-switched communications.[84]

5.3.1.1. The Skype service

Skype is arguably the most well-known peer-to-peer (P2P) VoIP service available with usage reaching 27 million simultaneous users at its peak. There is no separate server that manages the conversation between the two users in a Skype conversation, instead relying on the two (or more in the case of group-chats) users' computers to act as servers in the call.[85] The software and protocol that handles the call is proprietary, and it encrypts the call contents transparently, in the sense that users at no point need to know or have hold of the actual decryption keys used in the conversation. Lawful access measures put obligations internet service providers which are difficult to comply with in instances where technologies like Skype are used which prevent intelligible unencrypted from being accessed by law enforcement.[86]

Forced decryption provisions can become unenforceable requirements where the actual devices implement the encryption used in the conversation natively and outside of the direction of the users themselves. Italian law enforcement has raised the concern that all forms of crime have been turning to Skype and other VoIP platforms in order to avoid detection by investigators.[87]Anecdotally the investigators report having overheard a suspect

---

[84] Tomaz Aljaz & Franc Dolenc & Naim Maloku 'Legal call interception in next generation networks' (2003) 1 *Telecommunications* 47.

[85] Cheng & Lai op cit note 83.

[86] Law enforcement with the appropriate lawful access directive for a given interception would indeed be able to access the raw data that is transported during such a conversation, but would be at a loss as to access the keys necessary to decrypt it and make the conversation contents and possibly aspects of the traffic data intelligible. The key observation being that for a given warrant or authorisation, depending on the technology in use, law enforcement may find themselves unable to gather the actual data as they are empowered to, and would have attained in traditional circuit-switched networks.

[87] Joannes Thuy 'Eurojust coordinates internet telephony investigations' Available *http://www.eurojust.europa.eu/press_releases/2009/20-02-2009.htm* [Accessed 12 December 2010].

instruct an accomplice to switch to Skype so as to receive the details of a drug consignment.[88]

Liaising with the providers of the Skype service in advance of any interception attempts becomes a necessary step. However there are indeed a myriad of different service providers, each potentially with their own protocol and encryption method, making an un-standardised process very time-consuming and likely to fail in cases where timely responses are of the essence. The handover interfaces described in chapter 6 were developed by the European Telecommunications Standards Institute (ETSI) aim to streamline this process as far as possible.

5.4. Blackberry Service

Another notable Virtual Private Network is the Blackberry Internet Service and associated services like the Blackberry Enterprise Server and Blackberry Messenger. This proprietary service available on Blackberry devices is run by the Canadian mobile handset manufacturer Research in Motion. With 20 million Blackberry device users in the United States[89], a global market share of 14.8%[90] of all smartphones, RIM's device is both pervasive and iconic for its ease of use in mobile email and data communication as well as for traditional voice communications.

The sheer number of users as well as the widespread usage of these devices across a number of countries has made it a target from a number of quarters dealing with national security interests and local law enforcement. RIM describes the Blackberry Internet Service as "an email and Internet service for BlackBerry devices that is designed to provide subscribers with automatic

---

[88] Ibid.

[89] Comscore Mobile Mondays 'Top US smartphone platforms' available *http://www.comscoredatamine.com/2011/05/mobile-mondays-top-u-s-smartphone-platforms/* [Accessed 23 July 2011].

[90] Gartner Newsroom 'Gartner says worldwide mobile phone sales grew 35% in third quarter 2010; smartphone sales increases 96%' Available at *http://www.gartner.com/it/page.jsp?id=1466313* [Accessed 23 July 2011].

delivery of email messages, mobile access to email message attachments, and convenient access to Internet content."

Key components of the infrastructure are described as follows:

The engine	This application effectively acts as a post office, reconciling emails with addresses associated with that particular Blackberry device, both sending and receiving new email messages.[91]
Blackberry infrastructure	This is the portion of the Blackberry communications information system that physically belongs to RIM. Neither network operators nor corporations using the Blackberry Enterprise or Internet service have control over this portion of the system, meaning any lawful access measures necessarily impact on other portions of the network (specifically network operator or corporation controlled portions).[92]

[91] RIM 'Blackberry Internet Service' Available at *http://docs.blackberry.com/en/smartphone_users/deliverables/20443/BlackBerry_Internet_Service-Feature_and_Technical_Overview--1187001-0914104552-001-3.2-US.pdf* [Accessed 15 June 2011].

[92] Ibid.

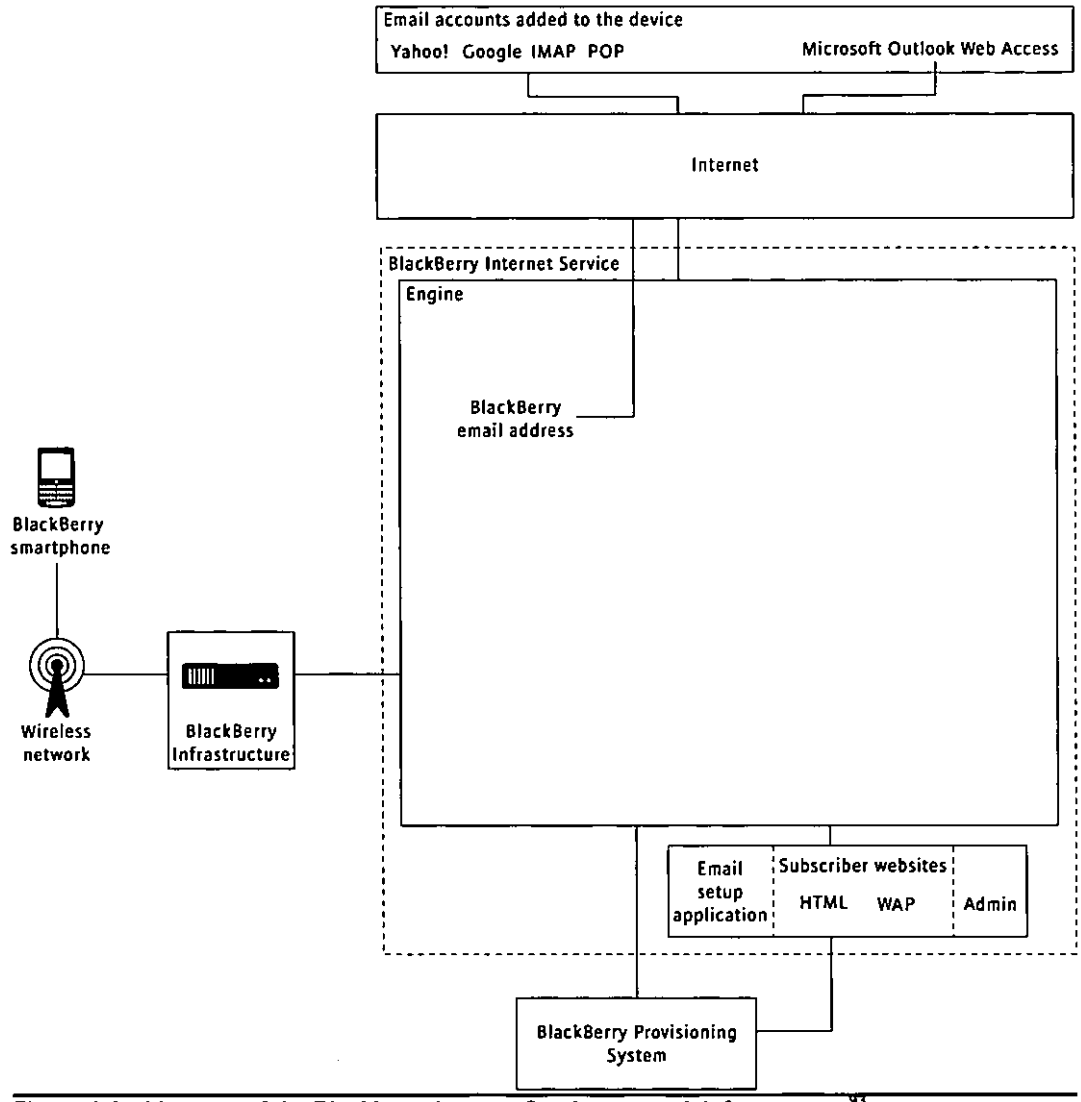

Figure 1 Architecture of the Blackberry Internet Service network infrastructure[93]

5.4.1. Fallout with national governments

In 2010 a number of countries raised concerns with the Blackberry devices and their encrypted communications. Among these countries were the India, Saudi Arabia and the United Arab Emirates which threatened to "block e-mail, instant messaging, and Web browsing on Blackberry devices"[94] if RIM failed to conform to their own domestic lawful access legislation and allow access to the

[93] Ibid.

[94] CNET News 'RIM responds to Blackberry ban in Middle East' Available at *http://news.cnet.com/8301-1009_3-20012478-83.html* [Accessed 10 June 2011].

encrypted services. The UAE cited the fact "that, in their current form, certain Blackberry services allow users to act without any legal accountability, causing judicial, social and national-security concerns" and '"...operate beyond the enforcement" of current telecommunications regulations in the country'. These governments insisted on RIM complying with lawful access requirements not just from the perspective of assistance in interception directions but also in the provision of decryption keys directly. RIM in turn asserted that their system simply has no master key or back-door access[95], with the customer's encryption key not entering RIM's or the network operator's control at any point during the transmission of data.

While RIM has made unspecified concessions, maintaining that all negotiations and agreements with states over lawful access are treated in confidence, it is clear that there are expectations that the status quo is untenable. An Indian governmental panel established to investigate the impact of security threats related to the use of several common forms of communications such as Skype, Gmail and Blackberry services determined both a short-and long-term strategy to deal with increasingly difficult lawful access enforcement.[96] The panel's conclusion was that "no service be banned purely on the grounds that it cannot be monitored"[97] which is commendable. Nevertheless, the limited extent to which the state security apparatus can exert pressure on foreign based firms for lawful access is acknowledged with short-term solutions including the installation of local servers in the country that must then conform with domestic lawful access measures, as well as interfaces for the sharing of encryption keys (Government access to keys) with authorized agents.[98]

---

[95] Ibid.
[96] The Times of India 'Gmail, Blackberry, Skype can't be banned: Panel' Available *http://timesofindia.indiatimes.com/tech/news/internet/Gmail-BlackBerry-Skype-cant-be-banned-Panel/articleshow/8885870.cms* [Accessed 25 June 2011].
[97] Ibid.
[98] Ibid.

Endorsed is the view that artificially limiting the level of encryption permitted in the country is an unnecessary risk that easier surveillance for law enforcement cannot justify. India currently only permits use of 40 bit encryption, while international standards sit at 256 bits.[99] Finally, the need to build domestic capabilities for surveillance is touted as a potential long-term goal.

Several commentators were quick to point out that the countries embroiled in the most recent assault on RIM's information system secrecy tended to be repressive regimes cracking down on dissenting voices; the sort that would be forced onto more secure networks like those offered on the blackberry platform, so as to avoid the strictly monitored public communications networks.[100] This concern however is slightly misplaced – in that societies viewed as "open" such as the United States and the United Kingdom have requested compliance by such telecommunications firms in the past as well. The overarching question is not *who* is requesting data, but rather *what* data is being requested and what mechanisms govern its treatment.

5.5. Online storage service provision

Also coming to the fore of lawful access, and interception debates is the issue of online storage facilities like Megaupload and Rapidshare. These services have been used on a massive scale to share files without the authorisation of the copyright holders. Users upload files to the server and provided with a link to the uploaded content, which they can then share with those they intend to distribute the file to. These services are somewhat distinct from more recent Cloud-computing based services or cyber-vaults in terms of their focus. These older file-hosting sites are geared towards the sharing of data, whether as video, music or other forms of media, with other users with access to an internet connection. Cloud-computing solutions of more recent times are primarily for the

---

[99] Ibid.

[100] Such as the Public Switched Telephone System (PSTS) or domestic internet service provider's email offerings, in contrast to services such as Google's Gmail or Yahoo, where interception requires the co-operation of parties not necessarily subject to the same interception regimes.

purposes of pervasive computing, allowing a single user to access their personal files from several different locations. The distinction is subtle yet important as these services battle for legitimacy online.[101]

From a technological point of view, interception in a Web 2.0 environment would have been very similar to the interception of traditional communications. This being law enforcement officers or a telecommunications service provider working under a directive issued to them monitoring the traffic of a customer suspected of using peer-to-peer (p2p) software to share copyrighted material. In the current regime, while uploading a movie to Megaupload would be considered an unauthorised copying of material, it could be treated as a fair use exception within the meaning of 'space shifting'.[102] Any interception warrant permitting monitoring of a target's communications would inevitably be limited to traffic being uploaded to the host (eg Rapidshare). Subsequent downloads of the material by other users would not be detectable without cooperation by the hosting site.

Any changes to existing interception regimes necessarily must take into account the substance of the actions that need to be prevented, rather than the form so as to avoid loopholes such as this. Similarly, very real questions of ISP obligations to monitor their network for infringements have become increasingly loud. The approach taken in the South African Electronic Communications and Electronic Transactions Act (ECT Act) strikes a fair balance, by respecting internet service providers' rights as businesses to function with as little

---

[101] While services like Megaupload have extensive terms and conditions ostensibly to prevent unlawful use of their services, these terms are more often than not flouted. Take-down notices though generally dealt with timeously are a symptomatic and aged method of dealing with infringing material that is uploaded with alarming rapidity. Groups representing the interests of artists and other rights holders typically work in an ex-post fashion, flagging material as infringing on copyright. In contrast, services like Apple's upcoming iCloud facility differ in that industry support will be established first, giving copyright holders the right to allow the use of their work in such systems.

[102] *Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc.*, US 1999.

hindrance from burdensome obligations to monitor. Nevertheless an exhaustive examination of specific copyright issues is outside the scope of this paper.

5.6. Encryption

Encryption, put most simply, is the codification of some text or information into a form that can only be decoded by those persons holding the appropriate decryption key to do so.[103] Its purpose is to add security to non-face-to-face communications by adding a layer of protection whereby should the encrypted communications (cyphertext) be intercepted the substance of the message remains secret to those not holding the key to decrypt it.

Encryption is employed in a wide range of everyday uses such as in securing communications in ATM transactions, internet banking and in the transmission of sensitive data such as credit card and banking details, passwords and other data of value.

In the analogue world, encryption could be as basic as re-mapping every character of the alphabet so that each corresponds to a different one to the original, and writing a letter using this algorithm. The intended reader would be made aware of the substitution in advance so that on receipt they are able to reverse the process thus deciphering the text. Naturally an encryption technique as basic as the one outlined above would be relatively straightforward to discover by those intent on intercepting such messages, so necessarily the stronger or more complicated the encryption measure the greater the guarantee of the safety of communications.[104] This is not to say that the communications

---

[103] Black op cit note 77 at 327.

[104] Another consideration is that repeatedly using the same method to encrypt quickly leads to lowered security as the interceptor is presented with more and more information required discovering the pattern. Once the pattern is discovered, not just future communications but all intercepted prior communications are compromised. Thus the health of innovation in the encryption industry directly impacts the safety of the data it is enciphers.

sent will not be intercepted, but rather that the data that is intercepted cannot be made into anything intelligible other than by the holder of the decryption key.

5.6.1. History of Encryption (brief)

Historically encryption has been the domain of military applications exclusively, emerging into common military use from the inherent lack of security in the use of radio communications.[105] The United States was quick to recognise the strategic advantage of being the sole holder of cryptographic techniques, and thus looked to put restrictions on the export of these methods. In an attempt to control their export outside the country encryption systems appeared on the U.S Munitions List (USML) as controlled by the Arms Export Control Act and Export Administration Act.[106] It was only in 1998 that a mechanism for the export of encryption systems of greater than 64-bits was created involving key escrow with the government.[107]

5.6.2. Key escrow

Key escrow is a system in which the keys necessary to decrypt encrypted messages are registered with the government or an approved body so as to allow the government to decrypt accessed communications on issuance of a warrant by the courts.[108] This system does differ in principle to that of forced-decryption, which has been adopted by the United Kingdom, where in the face of an order for decryption a target is made to decrypt some stored communications or provide their decryption key.

5.6.3. Applications and modern-day use

Access concerns for law enforcement have naturally led to a resistance to encrypted communications by consumers as it reduces their ability to monitor

---

[105] Black op cit note 77 at 334.
[106] Black op cit note 77 at 353.
[107] Ibid at 356.
[108] Ibid at 320.

conversations they otherwise would have had access to. At the same time advocates of more judicious encryption policy will argue that it is increasingly likely that commonly available computing tools are able to crack higher levels of encryption leading to security risks for users who rely on electronic communications but are legally barred from protecting their own use of these systems.[109]

Law enforcement and intelligence agencies have traditionally been the most vocal opponents of general access to high level encryption. What needs to be kept in mind is that the advent of Closed-Circuit Television systems did not usher in the end of the need for a door with a lock and key. Thus restricting the use of encryption through permitting only low-level encryption does not satisfy the underlying need for *actual* security of communications.

---

[109] Ibid at 334.
As illustrated by Black, a two-bit key is one where the key is made up of two characters, which can be either a 1 or a 0. Four different key combinations are thus possible: 00,11,01 or 10. As the key increases to say a three bit code (3 characters, again only either 1 or 0) then the number of possible key combinations increases, as does the security of the encoded text. This security is being eroded by the increasing processing power of computers which apply brute-force techniques, effectively constructing all the different possible keys until the correct one is successfully stumbled upon.

6. INTERNATIONAL STANDARDS IN LAWFUL ACCESS AND INTERCEPTION

6.1. Sources of Lawful Access powers

6.1.1. The Council of Europe's resolution on the lawful interception of telecommunications[110]

The Council of Europe's resolution on lawful interception established a set of protocols with respect to the requirements of legislation targeted towards helping law enforcement in their investigations where lawful access and interception were to be used.

Notable is that geographical locational determination was deemed a requirement in the case of 'mobile subscribers'. Information gleaned from traditional interception requests when dealing with fixed-line telecommunications operators inherently provided the sort of geographical information envisioned in the resolution. Owing to the fixed nature of the telephone system, law enforcement could be certain of not just the area but the specific street and building from which communications were recorded. The spirit of this resolution looks to be an attempt to preserve these exact powers even in evolved networks where communications devices can be mobile as well. This remains a key point of divergence in terms of policy between Europe and the United States, with the latter generally preventing the storage and accessing of locational data for lawful access purposes.

Features of the resolution that are present in existing lawful interception legislation include non-disclosure requirements[111] as well as an obligation to segregate non-target communications from target-communications in compliance with an authorized interception direction.[112]

---

[110] 1995.
[111] Section 5(1).
[112] Section 1(3).

6.1.2. The G8 and G7 resolutions

In 1996 the G8 focused its efforts on technological advancement and the effect it has on national efforts to fight terrorism and related criminal acts. The need to have effective multilateral agreements that function to facilitate prevention and investigation of these acts through access provisions was acknowledged, as well as importantly the 'protect[ion of] the privacy of legitimate communications.'[113]

6.1.3. The Convention

The Council of Europe drafted the Cybercrime Convention as a means of harmonising national laws on computer-related offences as well as the collection treatment and investigation of evidence that is electronic.

The stated aim of the Convention is for the "protection of society against cybercrime" by criminalising certain computer-related acts.[114]While aiming to tackle criminal activities of a broader sort, the Convention reflects much from the central aims of G8's principles and themes on computer-related crimes. The Convention establishes the following aims:[115]

- Harmonisation of substantive law across signatory states
- Harmonisation of procedural powers
- Creation of a sufficiently expeditious and effective process for mutual legal cooperation

Article 3 provides for Lawful access and lawful interception obligations:

> 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with

---

[113] Hosein, Ian op cit note 79 at 26.
[114] Michael A. Vatis – 'The Council of Europe Convention on Cybercrime' Available at *http://www.cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf* [Accessed 17 June 2011].
[115] Hosein, Ian op cit note 79 at 27.

dishonest intent, or in relation to a computer system that is connected to another computer system.'

Similarly, Article 10 criminalises the wilful infringement of copyright and related rights when the acts are "on a commercial scale and by means of a computer system".[116]

6.1.3.1. Data retention or preservation in the Convention

Data preservation and the enabling of real-time monitoring and wiretapping are explicit requirements of the Convention. Interestingly transactional data retention[117] is not a requirement however some jurisdictions such as the United Kingdom have enacted legislation requiring retention of records.

Article 20 and 21 call for adoption of measures to allow authorities to:

a 'collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of [different data types]'

Article 20 refers to traffic data in the while Article 21 refers to content data, where data is provided in real-time, associated with specified communications in its territory transmitted by means of a computer system.

Parties to the treaty are to ensure that requests for real-time data are kept confidential by the party obliging to it. These powers are nevertheless subject to the provisions of Article 14 and 15, thus still requiring that any lawful interception measures be limited in scope and be backed by adequate judicial or independent supervision conditions and safeguards.

---

[116] Vatis op cit note 114 at 212.

[117] Hosein, Ian op cit note 79 at 28.

6.2. ETSI Handover interfaces

The European Telecommunications Standards Institute (ETSI) produces standards for the ICT (Information Communications Technology) sector[118] and acts as an independent non-governmental organization. ETSI is recognized by the European Standards Organisation as a standards-setting body for the European Union.

Following the 1992 split of the AT&T monopoly in the United States, law enforcement began to struggle with fulfilling and operating under their requirements for lawful interception as instead of dealing with one service provider under a standardized process, interception now required the coordination of a multitude of service providers in the more open competitive market.[119]

Streamlining and standardizing the interaction between law enforcement and telecommunications service providers was imperative. The development of the ETSI Handover Interfaces (HI) for lawful interception has provided a flexible framework that has been adopted by a number of countries in fulfilment of coordinated mutual assistance requirements. The generic handover interface essentially categorises and separates each kind of action associated with lawful interception into three logical parts.[120] The resultant system is one that is applicable, though with some extra care required on the LEA's part, even to more complicated IP-based network interception.

---

[118] ETSI is an industry body overseeing telecommunications in Europe inclusive of fixed-line, mobile, radio, converged, broadcast and internet technologies. For more see *http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx.*

[119] Landau, Susan op cit note 80.

[120] ETSI 'Lawful Interception (LI); Handover Interface for the lawful interception of telecommunications traffic' (2007) Available at *http://pda.etsi.org/exchangefolder/es_201671v030101p.pdf* [Accessed 17 November 2010].

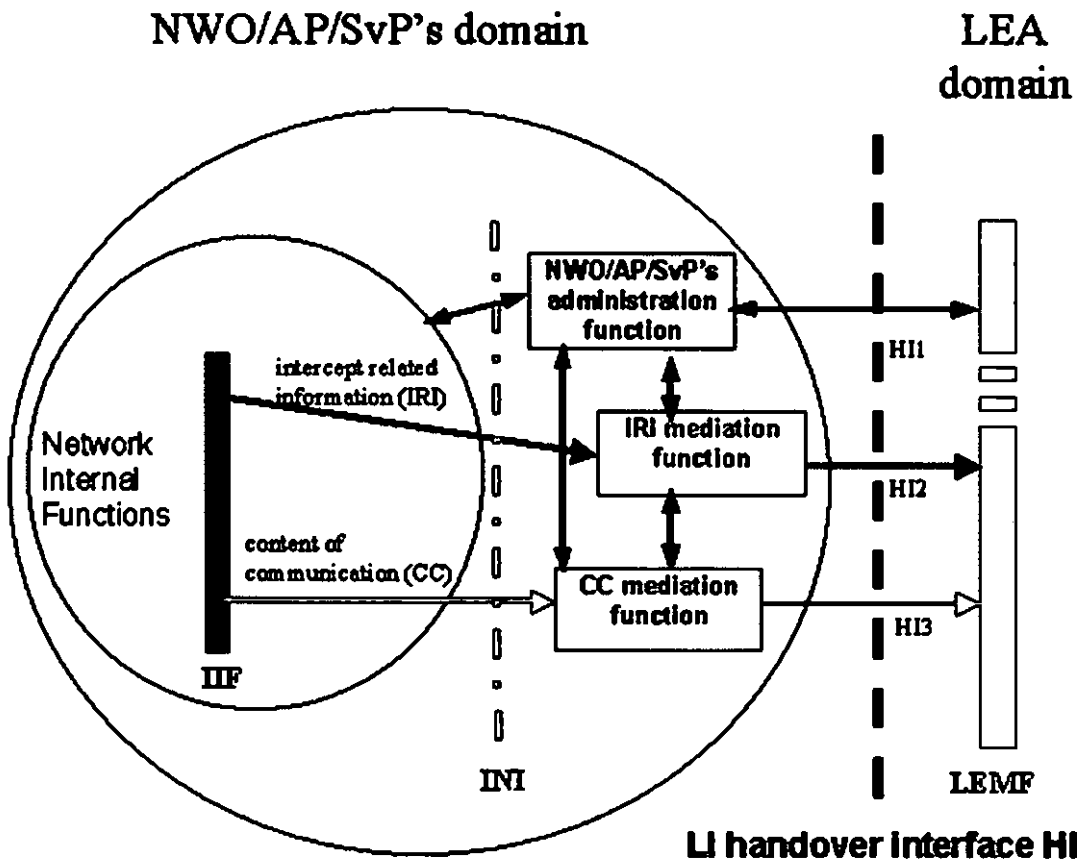

Figure 2: Functional block diagram showing generic Handover Interface[121]

The outer circle is the essential domain of control of the Network operator (NWO), Access Provider (AP) or Service Provider (SvP) with respect to lawful interception.[122] The Internal Interception Functions (IIF) provides both the Intercept Related Information (IRI)[123] and the Content of Communications (CC)[124]

---

[121] Ibid.
[122] Ibid.
[123] This is otherwise known as "traffic data'.
[124] Other terms commonly in use include call data, communications data or call content.

HI 1 - Administrative function

This interface governs the administrative function of LI,[125] involving transporting information between the communications organization and the LEA in question.[126] A key point to note is that only the communications provider has access to the actual interception switching function[127] and not the LEA, as the obligation under most LI regimes is to provide for interception capabilities- and not necessarily to have the LEA administer or access these capabilities directly. Similarly the administrative function and the technical part (The Internal Network Interface: INI) must be kept separate.

The sorts of messages interchanged in this function would be warrant statuses stipulating whether each is active or loaded, deleted or suspended and so forth.

HI 2 – Intercept Related Information function

This is more commonly known as traffic data, with all "events" related to call and or communication in and out of a specific target's device logged. Examples for a telephone call's intercept related information would include data such as "call received", time call received, length of call, time of termination of connection, as well as the caller's phone number.[128]

HI 3 – Call Content function

---

[125] There are specific identifiers applicable to all three interfaces which also apply to all communications methods and technologies that help identify target profiles (eg 'suspect X') with their associated interception data. The following are general identifiers applicable to all technologies:

Lawful interception identifier (LIID) – Essentially a unique identifying string that identifies a specific target, or a group of targets from a single interception investigation or subject, which is used commonly by both the LEA and the communications carrier.

Communication Identifier (CID) – Specifies an identify for each activity of a target.

See ETSI ES 201 671 V3.1.1 ETSI Standard on Lawful Interception (LI)

[126] ETSI op cit note 120.

[127] Ibid.

[128] Ibid.

This interface deals with delivery of call content or communications content, delivering the sort of data that old-fashioned wiretaps produce.

As explained in Chapter 5, interception of access networks and in particular circuit switched networks is relatively straightforward as all information transmitted in a particular connection is merely relayed or recorded for study by the LEA. In packet-switched networks, which are by their nature connectionless, this becomes rather difficult to do with acceptable levels of specificity, proportionality and minimization, as *all* packets must be examined[129] in search of packets destined for known IP addresses[130] of targets even in best-case scenarios.

6.2.1. IETF and IP networks interception standards

The Internet Engineering Task Force (IETF) is an open standards organization dealing in internet technologies and protocols with the goal of 'mak[ing] the internet work better' through influencing the "design, use, and manage[ment of] the internet'.[131] The IETF decided against setting technical standards for lawful interception on the internet.

6.2.1.1. Refusal to set standards for lawful interception

The IETF's refusal to set these standards is understandable. Research had demonstrated that any protocols that include wiretapping capabilities by design are inherently less secure than those without.[132] Creating such standards would be to impose architectures that are by design less secure than they could be which would compromise the security and integrity of these systems. Given the level of integration and dependence on internet technologies even by key

---

[129] Other complications such as IP tunnelling allow IP packets to contain other IP packets. See Philip Branch 'Lawful Interception of the Internet' (2003) 1 1 Australian Journal of Emerging Technologies and Society at 45.

[130] IP addresses can often be dynamically assigned by a DHCP server, meaning that warrants based on IP addresses lack the same effectiveness as those assigned to say a specific telephone number.

[131] IETF 'Mission Statement' Available *http://www.ietf.org/about/mission.html* [Accessed 18 November 2010].

[132] Landau, Susan op cit note 80.

governmental and national information communications infrastructures, it would be folly to endorse a move towards standards that reduce overall system security.

As explained in RFC 2026[133] one of the key concerns is to ensure due consideration of the interests of all affected parties, as well as establishing consensus across the community while evaluating the utility of the standard or specification for the internet. By leaving the debate up to national legislation and bodies, the IETF has washed its hands of the problem, opting "not [to] attempt to exert control over it, even though it may at times touch or affect the Internet."[134]

With the ITF silent on lawful enforcement standards two opposing effects have been observed. The first of these effects is the lack of standards adding to the uncertainty of service providers in terms of the best lawful interception capabilities to implement. Compliance is costly in terms of equipment and training, meaning service providers are faced with business risks that cannot easily be resolved. Given the differing nature of the treatments across jurisdictions this can mean the installation and maintenance of an array or hardware and software based controls that may not ever be called into actual use. There also remains the risk of receiving an order to install a certain capability that depending on the situation can be both expensive and have a negative impact on service provision in an industry where down-time is kept at less than 0.1% of the time per year.[135]

The second effect is that a lack of a standard increases security and integrity as having a variety of access capability ecosystems means less chance of a hacking group gaining access to the system through a uniform exploit that would then cause systemic security compromises across the board.

---

[133] Section 1(2).
[134] Ibid.
[135] My Hosting Reviews 'What is a network uptime guarantee and why is it important?' Available at *http://myhostingreviews.com/network-uptime-guarantee.htm* [Accessed 17 July 2011].

As explained in Chapter 2, the architecture of the internet and next-generation networks built upon the internet protocol would need a fundamental redesign in order to allow for the required level of reliability in interception needed by law enforcement.[136]

[136] Landau, Susan op cit note 80 at 31.

7. THE LAWFUL ACCESS REGIME IN THE USA

7.1. Context

The United States does not have a single comprehensive lawful access and interception statute as exists in South Africa and the United Kingdom. Instead it relies on the interaction of several pieces of legislation enacted at different points in time to fulfil these purposes. The Communications Assistance for Law Enforcement Act[137] (CALEA) provides the backbone for telecommunications carriers to make provision for lawful access capabilities and capacity, while the Omnibus Crime Control and Safe Streets Act's[138] Title III prohibits interception of communications. Title III was amended by The Electronic Communications Privacy Act of 1986 to include interception regulations for 'both digital and electronic communications...[and] new telecommunications switching technologies'.[139]

7.2. Title III interceptions

Title III prohibits the interception of 'wire, oral, or electronic communications', with exceptions being provided for in the case of operators and service providers and particularly in specific instances when used by law enforcement or other government officials backed by judicial authorisation. Intercept is defined as 'the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device'.[140]

To obtain a warrant an affidavit must be drawn up, showing probable cause that the targeted communications device is being used to facilitate a crime. The approval for the warrant is then granted by a member of the Department of Justice at least at the level of Deputy Assistant Attorney General, with the

---

[137] 1994.
[138] 1968 18 USC.
[139] Diffie & Landau op cit note 1 at 203.
[140] Paragraph 2510 (4).

completed application subsequently reviewed by a Federal district court judge. The criteria used by the judge in assessing the application are:

i) Probable cause to believe the individual is committing or is about to commit an indictable offence
ii) Probable cause that communications about the offence will be obtained through the interception
iii) Normal investigative procedures have been tried and either have failed, appear unlikely to succeed or are too dangerous
iv) There is probable cause to believe the facilities subject to surveillance are being used or will be used in the commission of the crime.[141]

All conditions must be satisfied in order for the warrant to be approved, and there is a closed list of offences for which interception of communications is permitted to be used in para 2516.

An order is approved for up to 30 days[142] with a requirement that interception cease upon the securing of the information needed to 'achieve the objective of the authorization'[143] with extension requiring a new court order. Congress requires records to be made available to the public whether under Title III or state statutes. A report must be filed with the Administrative Office of the United States Courts detailing the fact that an order or extension was applied for, its nature, duration, the offence in question and the outcome of the case and the identity of the applying officer or agency.[144]

In terms of the intercepted party's rights, after a period of at most 90 days after the conclusion of an interception (or indeed the denial of an interception request) it is left to the judge's discretion to have the target informed of the following:[145]

1) The fact of the entry of the order or the application;
2) The date of the entry and the period authorised, approved or disapproved interception, or the denial of the application; and

---

[141] Paragraph 2518 (3).
[142] Ibid (5).
[143] Ibid.
[144] Paragraph 2519 (1).
[145] Paragraph 2518 (8) (d).

3) The fact that during the period wire, oral, or electronic communications were or were not intercepted.

7.2.1. Pen register and trap and trace

Pen registers are electronic devices capable of recording the outgoing dialling information from a telephone line, while a trap and trace is capable of recording the details of incoming telephone numbers to a given telephone line.[146]Under ECPA both of these require court orders but not an actual search warrant, with probable cause not being a requirement for their approval.

The Patriot Act through para 216 greatly expands the definition of pen register and trap and trace to create a synthetic compatibility with Electronic Communications Privacy Act (ECPA) regulations on their use. Thus electronic communications eg surfing and email become open to the use of pen-register and trap and trace. Further, the opinion expressed in United States v New York Telephone Co[147] compounds the problem. The decision rejected the idea of an expectation of privacy on information derived from the use of pen registers. The assertion was that a pen-register 'does not overhear oral communications' while the reality of packet based communications is that both routing-information as well as content is contained, meaning the intercepter of these communications needs to be trusted to separate these two *ex post* interception of the packets.[148]

Even though interception using pen-register or trap-and-trace devices requires a court order[149], its issuance is subject to must less stringent requirements as compared to search warrants where probable cause must be demonstrated.[150] This treatment is particularly problematic when considered in tandem with the nature of certain kinds of traffic data that with astute analysis

---

[146] Jonathan Clough *Principles of Cybercrime* (2010).

[147] 434 US 159 1977 in Steven Osher 'Privacy, computers and the Patriot Act: the Fourth Amendment isn't dead, but no one will insure it' (2002) 54 *Florida Law Review* 521.

[148] Steven Osher 'Privacy, computers and the Patriot Act: the Fourth Amendment isn't dead, but no one will insure it' (2002) 54 *Florida Law Review* at 528.

[149] Ibid at 527 The court order cannot be denied where an applicant shows that the information requested is 'relevant to an ongoing criminal investigation'.

[150] *Smith v. Maryland*, 442 US 735 1979.

can yield telling information in a similar manner to content data which enjoys much greater legislative and administrative protections.

7.3. The Federal Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act[151] of 1978 (FISA) 'authorizes procedures for national security wiretapping' involving US persons residing in the US suspected of having links to international terrorism. It also requires a lower threshold of proof with no probable cause required in applications for authorization of interceptions. The reporting standards in FISA also fall short of those under Title III, requiring reports to the Administrative Office of the US Court of strictly limited breadth, providing detail on only the *number* of applications and the *number* denied by the courts. All other interception details are held as classified.[152] By 1995, over 8000 applications had been put processed, without a single application being denied.[153]

7.3.1. FISA and the Patriot Act

The Patriot Act further expands the reach of FISA regulations, by allowing not just communications with a foreign intelligence component, but also those declared to have a "significant purpose"[154] where "international terrorism or clandestine intelligence activities" are involved.[155] Passed in the month following the aftermath of September 11 2001, the Act's powers can be seen as a step backwards for the rights of those investigated, as the steeper Title III requirements gave way to expediency and the need to investigate and prevent terrorist activities *before* they occur.

---

[151] 1978 50 USC 1801.
[152] Diffie & Landau op cit note 1 at 202.
[153] Ibid.
[154] The Patriot Act s 218.
[155] Ibid s 214 (a) 1.

7.4. The Communications Assistance for Law Enforcement Act (CALEA)

The Communications Assistance for Law Enforcement Act (CALEA) was the first American legislative push to have interception capabilities built-in into the infrastructure of telecommunications carriers[156] such as digitally switched telephone networks.[157] In order to manage opposition from both industries to higher costs, as well as civil liberties groups to privacy concerns, the United States government attempted to strike a fair balance between continuing needs for surveillance capabilities and protection of privacy rights.[158]

CALEA was thus initially designed with a limited scope – to exclude so called 'information services' and apply only to 'telecommunications carriers'.[159] Accordingly, the requirement that intercept capabilities be provided for excludes those who provide "information services".[160]

The exclusion of 'information services' and private networks from the obligations to ensure interception capabilities was viewed by law enforcement as a glaring omission from the perspective of a cohesive and integrated lawful interception function. Criminals choose to use the medium that has the lowest level of risk of discovery available to them. Without a means of mandating interception capabilities for information services then services like VoIP and instant messaging take on the form of an unintended hotbed for both legitimate private use as well as abuse by those who wish their illegal activities to remain outside the watchful eye of law enforcement. Despite all the politicking that took

---

[156] Diffie & Landau op cit note 1.
[157] Landau, Susan op cit note 80 at 33.
[158] Hosein, Ian op cit note 79 at 20.
[159] This however is no longer the case. While 'information services' are still excluded, FCC rules have expanded the scope of telecommunications carriers to include broadband service providers as well as the providers of interconnected VoIP services. Electronic Frontier Foundation 'Communications assistance for law enforcement act' Available at *http://w2.eff.org/Privacy/Surveillance/CALEA/?f=summary.html* [Accessed 01 December 2010].
[160] CALEA s 102 (C).

place leading up to the enactment of CALEA the FBI as late as 1992 did admit to not having "'fumbled a criminal probe due to the inability to tap a phone...'".[161]

7.5. General provisions

CALEA sets up requirements for interception and monitoring capability, native to the system which is in contrast to operators providing assistance on a case-by-case basis.

Section 103 deals with the general assistance capability requirements of the act, setting expected standards of expeditious isolation and enabling interception of communications provided by telecommunications carriers. VoIP providers and broadband internet providers are now included subject to the FCC Order and Further Notice of Proposed Rule Making directive of 2005.[162] Such interception is required to be provided for regardless of mode of transmission, including 'all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier'.[163]

Section 103 (2) (A) provides for real-time isolation and access to call-identifying information that is 'reasonably available to the carrier'. Interestingly the specific data types required to be stored are not specified in the act, in contrast with the data preservation requirements in the United Kingdom that actually detail the kinds of data expected to be retained and preserved.[164]

Telecommunications carriers are not responsible 'for decrypting, or ensuring the government's ability to decrypt' any encrypted communications save for those that are encrypted 'by the carrier *and*[165] where the carrier possesses the information necessary to decrypt the communication'. This is

---

[161] Diffie & Landau op cit note 1 at 205.
[162] The Techlawjournal.com 'FCC Amends CALEA statute' Available at *http://www.techlawjournal.com/topstories/2005/20050805b.asp* [Accessed 18 June 2011].
[163] 103(a)(1).
[164] With specifications on how long each type of data is to be kept.
[165] Emphasis added.

significant in that telecommunications carriers as an integral part of the communications life-cycle need not be left open to the burden of decrypting communications where they were not directly involved in its encryption.

CALEA steers clear of setting any actual standards in terms of technology itself, instead allowing for three sources of directions and recommendations on the matter, being the FCC, industry and standard-setting organisations and most importantly the carrier itself. The flexibility provided is critical so as to allow normal business innovation and functioning, as well as to facilitate 'the policy of the United States to encourage the provision of new technologies and services to the public'.[166] CALEA provides neither recommendations nor prohibitions of specific equipment or manufacturers, instead simply requiring that the s 103 monitoring and interception capabilities and s 104 capacity requirements are respected.

The Attorney General was empowered to publish notice of the capacity requirements of law enforcement, with the FBI submitting requirements that set maximum capacity at over four times the annual number of phone surveillances.[167] The simultaneous interception capacity would sit at 30 000 lines. This called into question the sincerity of the agency and indeed the uses envisaged of the new capability requirements.

7.5.1.1. Carnivore

The Carnivore system was a system implemented by the FBI capable of intercepting and isolating specific data flows, allowing monitoring of email, browsing habits and chat conversations.[168]

Concerns were raised about the applicability of the Carnivore system even under CALEA as to whether transactional data capture can be kept separate from content data, when it is clear that a system like Carnivore would,

---

[166] Section 107(3)(b)(4).

[167] Diffie & Landau op cit note 1 at 221. This number is inclusive of Title 3 wiretaps, pen registers, trap-and-traces and FISA taps combined.

[168] Hosein, Ian op cit note 79 at 22.

in the process of gathering this information also potentially gather content data.[169] This would be in direct violation of s 103 (4) (a) which requires that the authorised interception of 'call-identifying information' had to be at the exclusion of communications data, specifically calling for safeguards to both the 'privacy and security' of non-authorised classes of data.

In 2000, The United States Congress heard arguments regarding the Carnivore system as an increasingly loud chorus of opposition rose against a system that was viewed as needlessly invasive, not sufficiently transparent in its operation as well as potentially damaging to the normal business functions of the systems it was attached to.[170] By the time of the initial hearing Carnivore had been used 16 times in the field, though apparently only for email communications[171] – the FBI was looking to expand its use to capture other forms of communications as well.

Throughout the hearing it became apparent that the normal operations of the system had it analyse all of the packets travelling through the node or point in the system where it was installed. These operations would occur in real-time, and would be tailored subject to the specifications of a warrant so as to intercept only the packets associated with the target's communications. Nevertheless the system had to trawl through a deluge of information unrelated to the target as well.

The analogy posited by Barry Steinhardt of the American Civil Liberties Union (ACLU) testifying at the congressional hearing provides chilling perspective in that the Carnivore system was akin to stationing an FBI agent at

---

[169] Congressman John Conyers rightly stated that, it is not appropriate to allow a device that collects a 'variety of data' to be used with pen register conditions, which authorize the collection of strictly traffic data. For more see Committee on the Judiciary's Congressional Hearing 'Fourth Amendment issues raised by the FBI's "Carnivore" Program' transcript available at *http://commdocs.house.gov/committees/judiciary/hju67305.000/hju67305_0f.htm* [Accessed 20 December 2010].

[170] Ibid.

[171] Kerr, D. 2000, Statement for the Record of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation on Internet and Data Interception Capabilities Developed by FBI as part of the Congressional Hearing.

'the Post Office ...and looking at the addressing information of every letter that goes through and then picking out those which it wishes to record, either the addressing information or to open up and actually look at the content'.

CALEA's specific requirement in terms of interception is that the means used provide isolation and interception of communications 'to the exclusion of any other communications' of a specific subscriber.[172] While at this stage there is legal uncertainty regarding what the interpretation of this clause is, it does seem plausible that a system like Carnivore and its subsequent replacement system, NarusInsight[173] which trawls through all the packets at a specific node, but only picks the ones that match the specific identifiers linked to the targeted subscriber, would be deemed as complying with the s 103 a (1) requirement.

Carnivore was installed into ISP systems to allow for monitoring. Astute hackers or criminals of any sort wishing to gain access to these records could arguably have pinpointed Carnivore as a possible point of vulnerability in monitored systems. Similarly, rogue law enforcement agents could in theory use the device to capture more than is authorised in the warrant, and in the case of agents particularly versed in the intricate programming of the device the audit trail ordinarily left behind by such changes and usage could be erased as well. From this perspective the public is rightfully concerned about the possible illegitimate use of such an invasive implementation in their communications systems. The Hepting v AT&T[174] case has highlighted the fact that these concerns are legitimate, following the discovery of illegal wiretapping access granted by carriers to government to facilitate illicit spying on huge swaths of the American population.[175]

---

[172] Sec 103(a)(1) of CALEA.
[173] Ellen Nakashima 'A story of Surveillance' Available at *http://msl1.mit.edu/furdlog/docs/washpost/2007-11-07_washpost_mark_klein_hero.pdf* [Accessed 20 June 2011].
[174] Ibid.
[175] Ibid.

7.5.2. ISP definition and responsibilities

As described earlier, CALEA refers to 'telecommunications carriers' as opposed to Internet Service Providers, with FCC rules expanding CALEAs reach to broadband providers and certain VoIP providers.

7.5.3. VoIP and CALEA

Nevertheless continued pressure from the FBI led to the Federal Communications Committee (FCC) announcement that CALEA's reach would extend to interconnected VoIP [176] and all facilities based, broadband Internet access providers.[177] The inappropriateness of this is startling given CALEAs requirement that government in the Justice Department effectively be in charge of setting technical standards, now to also be extended to standards for VoIP.[178]

Fall-backs to CALEA in the provision of interceptions capability by service providers like Skype,[179] or the Blackberry Internet Service appear limited. While in drafting there may have been some intent to remove the liability to provide interception capability from the telecommunications carriers themselves when providing access to additional services outside of their control[180] these provisions do not extend to information service providers as defined in CALEA, which both the Skype and Blackberry Internet Service would fall under. Similarly, not much can be made of the s 106's requirement for cooperation of telecommunications support services, as the definition of such support services

---

[176] Landau, Susan op cit note 80 at 27.

[177] The Techlawjournal.com op cit note 162.

[178] Landau, Susan op cit note 80.

[179] Robert Poe 'Can Skype Keep its Secrets' available at *http://www.voip-news.com/feature/skype-calea-compliance-061206/* [Accessed 26 June 2011]. As argued by Poe, Skype offers several different services, that function to allow peer-to-peer calling between Skype on individual computers and or mobile devices, while also offering SkypeIn and SkypeOut which 'permit[s] users to receive calls from, and place calls to, the public switched telephone network.' As per the FCC unofficial announcement of action, available at *http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260434A1.pdf*. These services are thus termed 'interconnected VoIP providers'.

[180] Such as the use of dial-up internet services, which rely on the telephone service provided by a fixed-line operator (the access network), which allows access to the actual value-adding service through the Internet Service Provider dialled into.

is relatively narrow and restricted to 'a product, software, or service used by a telecommunications carrier for the internal signalling or switching functions of its telecommunications network'. This leaves law enforcement with no recourse under CALEA for electronic communications interception assistance, however standard Title III and or FISA powers remain available to them.

7.5.4. Transaction data and traffic data

Referred to as 'call-identifying information' the definition is similar to that found in the Convention referring to 'dialling or signalling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.' As described in s 7.2.1 expanded rules on the definition of pen-registers and trap-and-trace devices have given room for lower thresholds of protection for call-identifying information.

7.5.5. Data retention/preservation

The United States has not adopted the same sort of data retention rules as has been done across Europe, instead opting to rely on data preservation. As noted by the Congressional Research Service opposition to data retention is a US policy issue, owing to a view that retention fails to strike the correct balance 'between the needs of law enforcement, business interests, and privacy rights'.[181] The ECPA[182], rather than CALEA regulates the procedural aspects of data preservation. The treatment differs not just in time periods of storage, but also in terms of the mechanism by which information stored is requested. Rather than a general obligation to store all communications information for a period of 6 to 24 months as in the EU Data Retention Directive, the ECPA provides for data to be preserved for a period of 90 days after a *specific* request by law enforcement.[183] The difference though subtle has significant implications

---

[181] Congressional Research Service 'Cybercrime: The Council of Europe Convention' available at *http://www.iwar.org.uk/news-archive/crs/10088.pdf* [Accessed 22 July 2011].

[182] Paragraph 2703.

[183] Kristina Ringland 'The European Union's Data Retention Directive and the United States Data preservation law: Finding the better model' (2009) the Shidler Journal of Law

for both businesses and users from cost and privacy perspectives. Electronic communications service providers need not preserve traffic data for users who are not subject to investigation. For users, their data will typically not be subject to blanket retention, and will at the expiry of the 90 days be subject to destruction, should law enforcement fail to attain the necessary court directive to access it.

7.5.6. Government access to keys

Owing to protections from Fifth Amendment rights against self-incrimination, there is yet to be a mechanism by which law enforcement can directly force decryption or the surrender of decryption keys of a person, even when in possession of a search warrant. Forced decryption was indeed on the cards at a point but it was shaken off during revisions of the CALEA bill. [184] This bodes well for privacy advocates, as the lowest power capable of requesting such keys or access remains in the hands of the courts or at a grand jury's discretion.[185]

7.5.7. Cost issues

CALEA does indeed establish a mechanism for reimbursement of some of the cost of interception capability measures.[186] Section 104 (e) provides for the reimbursement of costs incurred in insuring compliance with the carrier petitioning the Attorney General, who at his own discretion may agree to reimburse the carrier for 'such modification' required 'to attain such capacity requirement that are determined to be reasonable'. The approach as compared to that take in the United Kingdom does provide more certainty for operators affected by the law in terms of the criteria used to determine their financial need for assistance in compliance, as well as the commitment to assist with the financial cost.

Communication and Technology available at *http://www.lctjournal.washington.edu/vol5/a13Ringland.html* [Accessed 28 July 2011].

[184] Landau, Susan op cit note 80 at 27.

[185] Hanni Fakhoury 'Know your rights' available at *https://www.eff.org/wp/know-your-rights* [Accessed 28 July 2011].

[186] Hosein, Ian op cit note 79 at 29.

7.6. Conclusion

CALEA and subsequent amendments through the FISA amendment of 2008 and the Patriot Act are ostensibly aimed at preserving the investigatory and interception powers that law enforcement has, up until the advent of complex networks, always enjoyed. This contention is acceptable up until consideration of the associated reduction in safeguards and protections for the privacy rights of individuals that has also come along with it. This is aside from the necessary technical changes to the concept of interception and searches in packet-inspecting systems that the public has grudgingly come to accept.

From the perspective of industry standards and costs the role played by the FCC is ideal in the sense that the regulator would be best placed to understand the nature of the costs involved in capabilities provision. What is worrying is the extent to which the Commission seems influenced by law enforcement, seeming to bow to pressure for extraordinary capacity and capabilities above and beyond that envisioned by Congress when drafting the legislation.

The backdoor insertion of broadband internet providers into CALEA requirements is understandable given the difficulty associated with passing new surveillance legislation. Nevertheless the law of unintended consequences is in play, with failures in protecting certain types of data that skirt the boundary between being purely call-identifying (traffic) data or purely content-data. The Patriot Act's expanded definitions of certain surveillance devices has turned what are substantively digital searches into measures which aggrieved users have fewer defences against, and even fewer opportunities for recourse or notification of surveillance.

While the reporting standards that act as safeguards against continued abuse or frivolous use of interception mechanisms have been eroded over time the United States still retains one of the most comprehensive and inclusive systems of accountability.

8. THE LAWFUL ACCESS REGIME IN THE UK

8.1. Context

Interception regulation fell under the Interception of Communications Act[187] which followed the standard model establishing a general prohibition on interception of 'communications sent by post or by means of public telecommunication system'[188] with specific exclusions for the purposes of:

a) National security interests
b) Prevention and detection of serious crime
c) Economic well-being of the United Kingdom

These principles mirror the interests highlighted in Article 8 of the European Convention on Human Rights, while safeguarding the need to promote minimization requirements for the copying and retention of intercepted communications.

The Council of Europe adopted a stance that simplified the treatment of interception and searches, by referring to the collection of data that is in the process of being transmitted as interception, and stored or archived data collection as a form of search.[189]

8.1.1. Changes precipitating The Regulation of Investigatory Powers Act

Changing technological landscapes ranging from liberalisation in fixed line service provision to mobile telephone use ubiquity and internet communications technologies all gave impetus to drives to repair the silence of the Interception of Communication Act (IOCA) on key areas of communications surveillance.[190] A shift towards not restricting the possible forms that communications carriers might take saw the term Communications Service Provider (CSP) suggested

---

[187] Interception of Communications Act 1985 chap 56.
[188] Ibid.
[189] Murdoch Watney 'State Surveillance of the internet: Human rights infringement or e-security mechanism' (2007) 1 *International Journal of Electronic Security and Digital Forensics* 47.
[190] Home Office op cit note 35 at 2.

and eventually adopted expanding the previously narrow 'public telecommunication system' definition.[191]

The growing need of employers to be able to monitor the business correspondence of their employees was also recognized, given the requisite responsibility that employers necessarily take for the actions and correspondence entered into by their employees while at work.[192]

8.2. The Regulation of Investigatory Powers Act (RIPA)

RIPA read together with the Data Retention Regulations[193] rationalized the approach in the Interception of Communications Act, by opting to identify communications service providers (CSP); an umbrella term that encompasses internet service providers amongst the traditional mobile and fixed line telephone operators.[194] Other additions include provisions to cater for mutual assistance obligations with EU member states outside the UK, as under IOCA only requests from persons in UK territory were complied with.[195]

8.2.1. General provisions

Section 2(2) defines the meaning of interception of a communication as when 'in the course of its transmission by means of a telecommunication system if, and only if, he-

a) 'So modifies or interferes with the system, or its operation
b) So monitors transmissions made by means of the system, or
c) So monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,
d) As to make some or all of the contents available, while being transmitted, to a person other than the sender or intended recipient of the communication.'

---

[191] Ibid at 4.
[192] Ibid at 5.
[193] The Data Retention (EC Directive) Regulations 2009 no 859 Available at *http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksi_20090859_en.pdf* [Accessed 20 June 2010].
[194] Hosein, Ian op cit note 79 at 21.
[195] Home Office op cit note 35 at 19.

This treatment thus excludes devices like key-loggers which operate by monitoring keyboard keystrokes prior to transmission of the message, a relatively common method of illicit monitoring employed by computer hackers.

A significant departure from the approach taken in CALEA and the South African interception legislation is that RIPA requires capability installation and compliance only in the face of an s 12 notice from the Secretary of State of an interception capability requirement. There is no general compliance regime or standard, instead there is an obligation to comply with the specific requirements of an order.[196]

Monitoring under RIPA is permitted under the following conditions:

1) In the interests of national security
2) For the purposes of preventing and detecting serious crime
3) For the purpose of safeguarding the economic well-being of the United Kingdom: or
4) For the purpose...of giving effect to the provisions of any international mutual assistance agreement.[197]

8.2.2. ISP definition and responsibilities

ISPs are not excluded from the requirements of RIPA, as their offerings fall into the s 2 (1) definition of 'telecommunications service', thus demanding compliance of those who 'are providing public postal services or public telecommunications services' and those 'proposing to do so'. Private networks are thus exempt from the RIPA assistance and access requirements.

8.2.3. Transaction data and traffic data

The United Kingdom considers URLs content data, while the actual server address (for example 74.125.224.113 which is the IP address of Google.com) is seen as traffic data.[198] This is a positive move towards greater protection of

---

[196] Jeffrey Yeates 'CALEA and RIPA: the US and the UK responses to wiretapping in an increasingly wireless world' (2001) 12 *Albany Law Journal of Science and Technology* 125.
[197] RIPA s 6(3).
[198] Hosein, Ian op cit note 79 at 80.

sensitive data, however at the very same time, the UK permits a greater number of designated persons access to these data than other jurisdictions.[199]

8.2.4. Data retention/preservation

The United Kingdom was a major proponent of the new EU rules on data retention. The Data Retention Directive of 2006 requires that member states legislate for data storage requirements of minimum duration six months, and up to two years. This is in contrast to the previous requirements of about three months.[200] The United Kingdom provides for these requirements through the Anti-Terrorism, Crime and Security Act.[201]

The obligations are far-reaching, whereby anyone falling under the definition of communications service provider as defined in the Communications Act[202] In 2009 the potential liability arising from a failure to do so came to the fore as a pub-owner was fined £8,000 owing to the downloading of copyrighted material over the Wi-Fi hotspot operating in his establishment.[203] The obligations on the pub owner are to collect and store for a period of 12 months the communications data of all subscribers, and in this case, users of the Wi-Fi network. This communications data is as per s 2(b) of the regulations, the 'traffic data and location data and the related data necessary to identify the subscriber or user'. A typical internet café would most likely buckle under the pressure of effectively having to document and retain the details of every single prospective user – making their primary business of actual service provision redundant. It stands to be seen to what extent these regulations can be enforced outside of actions brought about by affected third parties such as in the case above.

---

[199] Ibid at 82.
[200] EU Data Retention Directive 2006 Article 6.
[201] 2001.
[202] 2003 s151.
[203] David Meyer 'Pub "fined £8k" for Wi-Fi copyright infringement' available at *http://www.zdnet.co.uk/news/networking/2009/11/27/pub-fined-8k-for-wi-fi-copyright-infringement-39909136/* [Accessed 27 July 2011].

America Online reported its estimates for establishing data retention systems at 30 million pounds, with a further 30 million pounds required annually to operate the system.[204]While s 106 (2) of the Anti-terrorism, Crime and Security act does make provision for reimbursement of costs incurred in complying with the data retention directive, it is not a requirement and remains at the discretion of the Secretary of State.

Perhaps the most worrying complication is the interaction between the obligations contained in RIPA when read together with those of the Anti-Terrorism, Crime and Security Act. RIPA provides for access to stored communications data by designated persons through s 22, while the Anti-Terrorism, Crime and Security Act contains requirements that oblige communications service providers to retain communications data (exclusive of communications content) of all users beyond normal business requirements for the purposes of national security. RIPA thus creates the unintended consequence of providing access to data collected for the express purposes of national security for purposes other than those envisaged.[205]

8.2.5. Government access to keys

Chapter III of RIPA allows law enforcement authorities to require the handover of encryption keys used in communications in a mechanism known as Government Access to Keys (GAK). This was one of the first forced decryption provisions among developed nations.[206] The justification posed for this stems from an interpretation of Article 19.4 of the Convention[207] requiring that:

"...any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as

---

[204] Ringland op cit note 183.

[205] The grounds provided in s 22(2), save for those in s 22(2)(a), are not in fact related to 'national security'. See Privacy International 'Anti-terrorism, Crime and Security Act 2001 Retention and disclosure of communications data Summary of counsel's advice' available at *https://www.privacyinternational.org/countries/uk/surveillance/ic-terror-opinion.htm#_ftn1* [Accessed 28 July 2011].

[206] Hosein, Ian op cit note 79 at 21.

[207] Cybercrime convention 2001.

is reasonable, the necessary information, to enable the undertaking of the measures..."

The implications for providers of communications security solutions are potentially damning. RIPA's forced decryption provisions[208] thus make an offence of withholding decryption keys from law enforcement, in stark contrast to the approach taken by the United States which upholds the rights of citizens against self-incrimination requiring an actual court order to gain access decryption keys.

8.2.6. Cost issues

RIPA's s 14 provides for the reimbursement of costs associated in securing the compliance with the duties prescribed in the act. The Secretary of State may at his discretion 'make arrangements for payments to be made out of money provided by Parliament'. This a much less solid commitment than that contained in CALEA for compliance. Further it is problematic that the Technical Advisory Board is the sole recourse for service providers wishing to appeal an order, given that the same board is one of the bodies the Secretary of State would have consulted prior to issuing the order. The Secretary of State's decision made with respect to any such appeal is then binding on the service provider as notice can be given 'confirming its effect, with or without modifications'.[209]

8.3. Recourse for aggrieved parties

Complaints relating to the conduct of intelligence services as well as interception of communications can be taken to the Investigatory Powers Tribunal, established in s 65 of RIPA. This is the sole forum through which aggrieved parties can lay complaints against wrongful use of interception. The powers held by the Tribunal are significant, as it can quash or cancel any warrant or authorisation[210] and or order the destruction of any records and data

[208] Section 48 and s 50.
[209] Section 12(6)(c)(ii).
[210] Section 67(7)(a).

held in relation to any warrant, authorization or person.[211] What is troubling is the unyielding lack of transparency in the process relating to informing the party involved of any interception or authorization granted. As pointed out by Hornle,[212] the Tribunal will either issue a statement declaring that it has failed to find in favour of the applicant, or that it has in fact found in the applicant's favour. The possible meanings in the former being that any interception involved was deemed lawful, or that there was no interception at all, and in the latter that the interception was unlawful. The lack of certainty as to the determination of the finding as well as the precise meaning of the possible findings prejudices the applicant in the interests of preserving the non-disclosure requirements enshrined in RIPA. This treatment is overboard in that the applicant remains ignorant of any of the details of even unlawful interceptions.

8.4. Conclusion

RIPA being one of the younger surveillance laws has the advantage of being the most comprehensive, leaving little uncertainty as to the range of entities to which it applies. This has, however come at the cost of establishing extremely broad and invasive powers open to quite simply, too many bodies, ranging from governmental departments, to local councils.

Forced decryption is at odds with rights to silence as well as right to avoid self-incrimination. Nevertheless there has already been at least on instance of this notice to supply decryption keys, and a failure to do so leading to a conviction in the UK.[213]

Protections against disclosure of interception authorisation by all the parties listed in s 19(2)[214] fail to create an environment conducive to the protection of

---

[211] Section 67(7)(b).

[212] Julia Hornle 'How to control interception – does the UK strike the right balance?' (2010) 16 *Computer Law and Security Review* 649 at 650.

[213] Chris Williams 'UK jails schizophrenic for refusal to decrypt files' available at *http://www.theregister.co.uk/2009/11/24/ripa_jfl/page2.html* [Accessed 10 June 2011].

[214] Where disclosure of the details of an interception warrant is made an offence and prohibited to members of the National Crime Squad, the National Criminal Intelligence Service, persons

privacy rights of citizens. This is not likely to change as even the European Court of Human Rights has confirmed that while Article 6[215] of the European Convention on Human Rights applied, national security interests and the withholding of dissemination of secret investigative methods was necessary.[216] The message to take home being: Trust us not to abuse these powers. Privacy advocates wary of previous infringements of these very rights will be quick to retort that such trust is yet to be earned.

---

holding office under the Crown, members of the police or postal services as well as those in the provision of or control of telecommunications services.

[215] Right to a fair trial.

[216] The court opinion in Hornle op cit 212 at 650.

9. THE LAWFUL ACCESS REGIME IN SOUTH AFRICA

South Africa prior to the end of apartheid faced strict monitoring with agents of the security apparatus using communications surveillance to observe the organising and canvassing activities of those deemed a threat to national security and the status quo. After 1994, legislative reform finally took aim at the old interception regimes in the country, and worked to protect the rights of citizens more comprehensively as well as to update the law to provide for greater empowerment of law enforcement in reducing the scourge of violent crime that has engulfed the country.

9.1. Context

In a similar approach to the United Kingdom, South Africa has enacted a single, broad surveillance act, The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).[217] RICA is aimed at establishing prohibitions on interception of electronic communications, as well as imposing capability requirements on providers of telecommunications services. Provisions defining the concept of electronic and data messages are found in the Electronic Communications Act.[218]

RICA repeals the former Interception and Monitoring Prohibition Act of 1992[219] and establishes what some view as a more up to date approach to lawful access and interception that should add to certainty within the industry despite a lingering dearth of applicable case law.

9.2. The Interception and Monitoring Prohibition Act

The National Party that governed South Africa right until 1994 slowly loosened the police-state controls it had implemented over time to quell subversive movements aimed at self-determination in the Republic.

---

[217] No 70 of 2002.
[218] No 25 of 2002.
[219] 127.

The monitoring of individuals linked to communist movements and other undesirables is well known and documented.[220] The National Intelligence Service (formerly the South African Bureau of State Security) and other law enforcement structures were authorised to act with relative impunity in the interception and monitoring of postal and other communications. The Interception and Monitoring Prohibition Act was enacted with a view to restore common law privacy rights[221] as well as a confidence in the non-interference by the state in the lives of individuals.[222]

The South African Law Review Commission (SALC) in their investigation and review of the Interception and Monitoring Prohibition Act concluded that any new act should place a more central focus on the detection and prevention of crime as well as national security interests. [223]

9.3. The Regulation of the Interception of Communications and Provision of Communications Related Information Act (RICA)

The Interception and Monitoring Prohibition Act was subsequently repealed by the Regulation of the Interception of Communications and Provision of Communications Related Information Act (RICA). The Telecommunications Act that defined 'telecommunications services'[224] was repealed by the Electronic Communications Act (EC Act). The EC Act does not define telecommunications services, but instead divides communications into conceptual groups, along broadcasting and general "electronic communications" lines, where the former is a "unidirectional" electronic communication and the latter effectively encapsulating all other forms of "emission, transmission or reception of

---

[220] Cohen op cit note 39.

[221] Ibid.

[222] Ibid.

[223] Nazreen Bawa 'The Regulation of Interception and Provision of Communication-Related Information Act' in Lisa Thornton et al (ed) *Telecommunications law in South Africa* (2006) 296-332 at 297.

[224] Where telecommunications service is defined as "any service provided by means of a telecommunication system", and a "telecommunications system" as "any system or series of telecommunications facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication...".

information" . The RICA amendment Act[225] has updated some, but not all of the references to telecommunications service providers, referring instead to 'electronic communication service provider' in accords with the Electronic Communications Act. This shift from a regime that tried to compartmentalize forms of communications along very strict lines resulted in an act that some viewed as prone to obsolescence owing to the unpredictable pace and direction of technological advances.

The growth in use of electronic mail, cellular communications amongst others highlighted technology neutrality as a key point to consider in any future revisions of the law. Rather than deal with labyrinthine treatments and categories of communications where the specific medium over which communications travels determines its particular interception requirements, the South African legislation has hewed communications in two. Communications are either direct or indirect, with indirect referring to any form of communications travelling over a 'postal or telecommunication system'[226] while direct effectively refers to face-to-face communications.

9.3.1. General Provisions

RICA establishes a general prohibition on interception[227] with s 3 providing for limited exceptions on interception in the cause of authorised persons executing interception directions. The definition of interception actually includes what was considered monitoring under the previous surveillance act, but does not stray far

---

[225] No 48 of 2008.

[226] A further problem in the internal consistency of RICA is that despite the attempts to update the legislation to reflect the definitions in the EC Act that repealed the Telecommunications Act, not all of the terms have been updated, making RICA dependent on certain terminology no longer in legal use.

[227] Section 2 with interception defined in s 1 as

> "any activity that allows for the acquisition of the contents of any communication...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"

at all from the definitions adopted in the UK. Interception according to s 1 refers to the

> 'aural or other acquisition of the contents of any communication 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 communication; and
> c. Diversion of any indirect communication to any other destination.'

This definition is limited to instances where a direct communication is intercepted during its occurrence and in the course of transmission for indirect communications.[228]Where RICA differs from most interception prohibition legislation is in the concept of parties to a communication, with *any* party[229] to the communication permitted to intercept and disclose the content and or communication related information.

Duties established for communications operators, identified as 'electronic communications service providers' in the EC Act[230] and the RICA Amendment Act, include the provision of interception capabilities that are to be installed, maintained and operated solely at the service providers own cost.

---

[228] RICA s 1(2)(a).

[229] RICAs definition of party would in practice extend the interception exception as far as an eavesdropper or passer-by who happens to intercept the communication save for when such interception is for the commission of an offence.

[230] The EC Act amends certain sections of RICA, substituting 'electronic communications service provider' for 'telecommunications service provider'. The RICA Amendment Act 48 of 2008 also makes similar adjustments to the remaining instances where definitions from the Telecommunications Act are referenced.

9.3.2. Exceptions to the general interception prohibition

9.3.2.1. Interception of communication by a party to the communicotion

An exception also exists for parties to a communication to intercept that communication in circumstances other than for the commission of an offence.[231] This exception however is qualified when dealing with 'law enforcement officer[s]' who have an additional burden of proof in terms of s 4(2)(b) where the grounds presented under 16(5)(a) must also be considered. These grounds are the facts that a designated judge considers in granting an application for an interception direction. A literal reading of RICA does imply that a party to the conversation is not obliged to inform the other party of the recording of any conversations where the recording is not to be used in the commission of an offence. The definition of party effectively encompasses anyone ordinarily considered to be a party to a conversation as well as some added particulars that seem to provide some internal inconsistency to RICA. In direct communications a party to the communication is defined as a person

1) Participating in such direct communication or to whom such direct communication is directed; or
2) In whose immediate presence such direct communication occurs and is audible to the person concerned, regardless of whether or not the direct communication is specifically directed to him or her.[232]

RICA as compared to the Interception and Monitoring Prohibition Act thus decriminalises spying in the case of direct communications by non-law enforcement agents where such a person is able to be in the immediate presence of the direct communications whether or not they are directed at him or her. This is likely to be reviewed in court as an overbroad outcome. What is important to note is that the legality of surveillance is a separate issue from admissibility in court. Thus the opinion held in Lenco Holdings Limited vs

---

[231] Section 4(1).
[232] RICA s 1 definitions.

Ekstein[233]that the court retains the discretion in terms of the admissibility of recordings still stands.[234] This discretion might become an ineffectual protection however, as the discretion is exercised only in cases where s 4 exceptions are not applicable.[235]

Section 4's exception can in some instances be at direct odds with the judicial precedent established in S v A. A private investigator recording a conversation while within earshot of it, whether noticed or not by the speaker would be permitted to do so under this exception. This is when the definition of a party to the communications is considered as including eavesdroppers who use no technical means of enhancing their hearing above normal hearing.

9.3.2.1. Interception of communication with consent of party to communication

Section 5's exception does seem compatible with previous court findings, but does seem loosely worded in such a way as to defeat the safeguards contained therein. Law enforcement officers have been provided with a mechanism within which to operate interceptions for the purposes of investigation. Section 5 (1) does exclude the provision of consent to law enforcement officers, with such officers needing to comply with s 5 (2)'s conditions. Law enforcement officers are thus enabled to commission non-officers such as private investigators to conduct interceptions on their behalf.

9.3.2.1. Interception of communication to prevent serious bodily harm

The prevention of bodily harm provision is unique in that no such express exception is provided for in the United States or the United Kingdom. As an exception to the general prohibition against interception, it thus is subject to the rules on limitation of rights in terms of s 36(1) of the Constitution. Determining its

---

[233] 1996 (2) SA 693 (N).
[234] Stimela Mokoena & Thokozile Zambane 'Sshhh - someone may be listening' (2010) 10 *Without Prejudice* 20.
[235] Ibid at 20.

constitutionality hinges on "'weighing up of competing values and ultimately an assessment based on proportionality"',[236] with the objects of the exception being compared against international best practice, the view taken in an open and democratic society as well as the preservation of human dignity, equality and freedom.[237] The interpretation of the limitation of constitutionally guarded rights is dealt with on a case-by-case basis. The exception can be invoked in situations where bodily harm has not occurred, referring to a future potential harm. While the objectives of the s 7 exception are arguably noble, the practical effects of the law may in fact leave it open to being reviewed in terms of its constitutionality.[238]

Officers invoking this section have effectively exercised the authority of a designated judge, a power which the act seeks to balance by providing for the review of interceptions carried out under such conditions. Section 7 (4) sets out these reporting requirements, that are then presented to a designated judge. Where there appears to be a failing is in paragraph (c) where the officer is permitted to self-assess the justification for the interception. The officer is required to furnish the designated judge with the full or partial transcript of the recording and notes only when the officer by his own actions admits the interception yielded nothing to suggest bodily harm and effectively admits fault. An officer couching the results and information obtained in language that relies on suggestions or mere implications of bodily harm thus escapes potential liability for unauthorized interception. There is no mechanism within the act to keep in check or stem the number of false-positive errors, where officers mistakenly err on the side of suspicion under s 7.

---

[236] *Prince v President of the Law Society of the Cape of Good Hope* 223 2002 (2) SA 794 (CC) para 45 and *S v Jordan* 2002 (6) SA 642 (CC) para 85. in Bawa op cit note 223 at 306.
[237] Ibid.
[238] Ibid at 320.

A similar approach has been taken to deal with determining locational data 'in case of emergency'[239] under s 8. Such interception is to be requested by a law enforcement officer when informed of such a situation.

What needs to be kept in mind is that s 7 and 8 do indeed serve a useful function, especially given the conscious acknowledgement in 7(b) of the need to be able to respond quickly in urgent situations. Nevertheless more thorough judicial review is needed when presenting such a broad limitation of constitutional rights to privacy.

9.3.2.2. Interception of indirect communication in connection with carrying on of business

Workplace monitoring is specifically dealt with in RICA. Businesses are permitted to monitor the communications sent using the businesses communication services subject to the conditions set out in s 6 of RICA. Most businesses will rely on a system that requires employees to acknowledge that they understand that the primary use of these services is for business purposes,[240] and that the use thereof is subject to monitoring. This often takes the form of a login page where failure to accept the terms of use prevents use of the workstation.[241] The term consent likely takes a less strict interpretation as compared to the concept of consensus in the law of contract, but remains problematic in the sense that the employer will require use of the workstation to fulfil one's role, limiting scope for consent to be freely given.

RICA does provide an effective means for workplace interception, while balancing the needs of employees to expectations of privacy even when

---

[239] An emergency is described as any set of circumstances where the life of any person party to communications is in either present or potential risk, as well as where there is risk of serious injury.

[240] Section 6(c) of RICA which states that the electronic communications 'system concerned is provided for use wholly or partly in connection with that business' which shows cognisance of the possibility that employees might use these services for both business as well as purposes other than those in the ordinary course of business such as personal communications.

[241] This is normally done with a view to fulfil the requirement for 'express or implied consent of the person who uses that telecommunications system' as per s 6(2)(d).

communicating at work. The range of circumstances where an employer would be criminally liable is sufficiently narrow.[242]

9.3.2.3. Other interception exceptions

Further exceptions include s 9's reference to the interceptions authorized under the Correctional Services Act[243] as well as monitoring of signals for the purposes of installation and maintenance of equipment or facilities used in connection with a communications service. The thinking behind this is to prevent over-criminalisation given the broad ambit of RICA's general prohibition, which would have prevented even legitimate monitoring in the maintenance and normal provision of services by operators. In a similar fashion an exception for monitoring of signals for spectrum management is provided for in s 11.

9.3.3. Directives in terms of section 30 of RICA

Section 30 of RICA requires the Minister of Communications to issue directives relating to the manner in which authorized interception will be conducted, the 'security technical and functional requirements of the facilities'[244] as well as the type of communication related information to be stored by electronic communications service providers[245]. These directives were issued in November of 2005, with all service providers required to ensure compliance within six months.

The directive though providing guidance on the required interception capabilities of communications service providers does not have as great an impact on the key privacy questions around RICA. An example being the capability to collect and store RADIUS login data, which as explained in s 4.3 can inadvertently provide locational data even in cases where an interception direction might not permit or require this information. The capability of the

---

[242] For a detailed discussion on workplace interception the circumstances where workplace monitoring would lead to criminal liability under RICA see Steven Ferguson *The monitoring of e-mail and Internet usage in the South African workplace – The final word* (2002) at 44.
[243] Act No.111 of 1998.
[244] (2)(ii).
[245] (2)(iii).

interception related systems is not the area of concern as much as the actual interception direction and or warrant, which define the precise information that is to be excluded or included in fulfilling each direction. What fundamentally influences the appropriateness and proportionality of directions is the underlying enabling legislation which determines the level specificity of judicial warrants and interception directions to be applied.

RICA does not provide guidance on the precise data types that can be collected. What RICA does do is to provide two distinct mechanisms that law enforcement can pursue, as either an application for 'communication-related direction'[246] or an application for 'interception direction'. Interception directions provide access to both communication-related data as well as the actual content data of a communication, while communication-related direction provides data that conforms to the s 1 definition of 'communication-related information'.

It should be clear that applications granted in such a regime will provide access to overly broad data types. By way of example, if one compares the data accessible using a 'pen register' in the ECPA Title 18, where numbers called from a specific phone line are recorded, with the data accessible through a duly issued communication-related direction, it is clear that there is no obligation to limit the data to a specific kind (eg outgoing calls dialled) providing a general inspection of all communications-related information. This failing is systemic in that while communications service providers are required to limit the information they provide to the specifics of the direction received, the direction itself is not subject to specificity requirements, rendering the service provider safeguard nugatory.

9.3.4. Conditions and safeguards

Currently, no form of reporting standard or requirement is contained in RICA. Both the United States and the United Kingdom have annual reports presented to the Administrative Office of the United States Courts or required of the

[246] A number of categories exist under 'communication-related direction' including s 17's real-time directions, s 19's 'archived' data as well as combined applications under s 18.

Interception of Communications Commissioner. In South Africa, while the Minister might be empowered to impose public reporting requirements of the Director of the Office for Interception Centres, no such requirement exists in the act. Indeed RICA contains no objects to compel the Minister to consider public reporting standards.

9.3.5. ISP definition and responsibilities

Internet service providers are not exempt from RICA's reach, and are singled out in terms of their obligations, with an additional requirement to contribute to the Internet Service Providers Fund if exempted from s 30(4)[247] requirements by the Minister.[248] Envisioned as qualifying for this exemption would be smaller ISPs which owing to financial constraints cannot provision for extra equipment and or the technical expertise needed for interception capability. In such a case, any law enforcement agency bringing forward applications for interception will be required to make the necessary facilities and devices available to execute the direction.

The Internet service provider definition in RICA, and its subsequent amendment in the EC act is too broad. The obligations to provide for lawful interception capabilities as well as subscriber registration then extend as far as universities and even employers that – 'provide[s] access to, or any other service related to, the Internet to another person'

9.3.6. Transaction data and traffic data

Communication related information is the term adopted in RICA to refer to 'any information relating to an indirect communications...[detailing] switching, dialling or signalling information that identifies the origin, destination, termination, duration and equipment used'[249] in the indirect communications, as well as 'the location of the user within the telecommunication system'. This approach is

---

[247] Section 38.
[248] The Minister of Justice and Constitutional Development.
[249] Section 1.

identical to that taken by the United Kingdom, in that locational data is also considered an essential part of traffic data.

Nevertheless there is overwhelming uncertainty in terms of the specific data types that are considered to be switching, dialling or signalling. There remains no direction as to whether URLs would be treated as content data (ie not communications related data). It appears that a bare minimum would be the collection of the IP addresses of websites accessed under these requirements. While it remains to be seen if this is the case in practice, the implications are grave. As demonstrated in chapter 4.3 of this paper meticulous analysis of data such as IP addresses and indeed web searches can reveal a great deal of information, giving it a quality akin to content data, and at least in theory necessitating a higher threshold of justification to access it.

9.3.7. Data retention/preservation

RICA does not expressly classify its position on the storage of data as preservation or retention. Functionally however, the imposition of data types to be stored as well as the length of time for which it is kept makes RICAs treatment one of data retention; ie retention above and beyond the lengths of time required for business as mandated by government.

While the meaning of communication-related information has been defined in the Act, the Minister is still empowered to determine the type of communication-related information that is to be stored, with minimum windows of three years, and a maximum of five years. These periods of data storage stretch significantly further than even those stipulated in the United Kingdom. Communications service providers have consistently complained of the serious impact of lengthy retention requirements. Those provided for under RICA would make South Africa one of the most hostile places to do business in the world in terms of data storage obligations.

9.3.8. Government access to keys

Section 51 (4) makes an offence of a failure to comply with decryption directions with penalties ranging from fines not exceeding R2 million, or imprisonment for a period not exceeding 10 years, or for juristic persons fines up to R5 million. This places heavy burdens on holders of decryption information in an environment where proposed data protection laws[250] also create offences of certain kinds of disclosure of data. Further, any person convicted of this offence is still obligated to produce the decryption key. The penalties for the refusal to disclose decryption keys to even one's own data are the same as those applied to an illegal and unauthorised interception of the communications of other parties.

9.3.9. Cost issues

Save for the exemptions afforded ISPs in particular, the Minister has failed to Gazette tariffs[251] to address the issue of cost-sharing or reduced burden to operators who comply with RICA's capability obligations.[252] Given the fact that the Minister determines the 'security, technical and functional requirements of the facilities and devices to be acquired by the' communications service provider, it is puzzling that such an inflexible regime such as uniform tariffs has been chosen. Meanwhile further obligations have been put on mobile operators in particular, who under s 62A are required to compensate 'persons employed to record and store the information contemplated in s 40 and s 62(2)' related to

---

[250] See the Protection of Personal Information Bill. It is possible however that the actions in compliance with RICA may be passed as exceptions to these rules. The question of the sort of benefits that qualify as a 'substantial degree' will be raised even in the context of RICA decryption directions.

[251] Section 31.

[252] Compliance here taken to mean installation of interception capabilities and capacity. The Minister of Justice has in fact gazetted a compensation scheme for mobile and fixed-line operators for their *assistance* in complying with interception directions. The cost of installation of interception capabilities and capacity thus still bears solely on the operator themselves. See regulations in GN R93 and R94 *GG* of 6 February 2009.

registration of sim-card owner details. The uniform rate has been determined at R3.00 per sim-card.[253]

Effectively the government has imposed a tax on communications service providers that subsidises its own surveillance requirements. Until such time as the tariffs are determined it is possible that these costs will be passed on to consumers in some form or other. This added to the imposition of the Minister as de-facto role of standards-setter through the prohibition of the 'possession, assembly, purchase or advertisement of listed equipment' further calls into question to what extent the co-operation of communications service providers is actually valued in this process.

9.3.10. Privacy concerns

South Africa though yet to ratify the Cybercrime Convention, has in principal agreed to enact laws that conform to the minimum standards set about in that treaty. Article 15 prescribes that states provide for:

> 'Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.'

South Africa given its long history of state abuse of power has done well to create judicial safeguards, where requests for surveillance are decided either interception requests or purely communications-related information, the threshold for the former being higher. What is lacking is independent supervision by an independent body or organ of state that is not affiliated with any law enforcement agency. The submission of annual reports on purely numbers of directions applied for and approved would help to drive transparency.

---

[253] Determination of uniform tariff of compensation payable in terms of s 62A regulations in GN R1121*GG* 32759 of 27 November 2009.

9.3.11. Other points of contention

'Roving wiretaps' as they are known in the United States are pen-registers and trap-and-trace orders that need not specify the exact location where monitoring is to take place, the introduction of which was not without opposition. The motivation behind allowing non-location specific applications for surveillance likely lies in the increased popularity of mobile devices like cellular phones and indeed pervasive internet access. The concern is that principles of minimisation and exclusion of other communications are impacted by a failure to provide for the exact location of required interception. The act needs to require applicants to provide justification for a location-agnostic direction, rather than the current standard which merely recommends location specification.

9.4. Conclusion

Ironically at no point in the act is the word privacy used either literally or in its constitutional concept. The objects of the act describe aims that serve the state security structure exclusively without any commitment to upholding the rights of private individuals.

RICA is yet to be extensively tested before the courts, however given its multiple failings to respect constitutional safeguards it does seem likely that it will come under review at some point in the future. Proportionality principles though mentioned in passing in the legislation are not enabled as the reality of the data requirements demanded of electronic communications service providers is at odds with any form of limited and targeted investigation of communications. The burdens placed on electronic service providers and in particular ISPs are manifold making compliance with RICA costly and difficult. The consolation that consumers can draw however is that enforcement of these requirements is equally burdensome, making wholesale compliance something of a pipedream.

The powers bestowed law enforcement officers though tempered by judicial oversight in some instances fails to provide adequate safeguards by

providing alternative means of interception by the same officers through the use of exceptions such as s 5 and 7. Thus even the limited judicial review provided for by the act is curtailed by the selfsame.

Also of interest is the fact that South Africa on ratification of the Council of Europe's Cybercrime Convention will be required to bring RICA in line with obligations under the treaty, addressing failings ranging from overbroad powers and insufficient levels of "conditions and safeguards" in the powers and scope of application of lawful interception regulations as well as a worrying lack of public review of interception directions and indeed recourse for parties whose communications are intercepted lawfully.

RICA did provide the government with an opportunity to distance itself from the previous regimes disregard for civil liberties and strike a fair balance between national interests and the rights of citizens. The act has not done so adequately, and has in fact cemented perceptions of a general spying agenda by government. The legislation grants powers to authorised persons in a way that implies a desire to implement pervasive monitoring, while the lack of public reporting requirements betrays a desire to ensure such monitoring remains hidden.

10. CLOSING COMMENTS

New technologies have changed the way people communicate and do business. Fundamental differences in the nature of circuit-less IP based networks as compared to older exchanges like the plain old telephone system (POTS) have made it impossible to approach interception and lawful access in the same ways as before. Lawful interception techniques adopted to allow for continued investigative powers have raised an important point for society as a whole.

It is possible that users will have to come to accept that in some shape or form, all our packet-based communications will be subject to search. Semantics and posturing can indeed make it so that systematic checks of packets aimed at segregating target communications from non-target ones are labeled as something other than a 'search'. The fact of the matter remains that some compromise is needed in order to give effect to lawful access requirements. If and when such an understanding is reached, then civil liberties groups and privacy advocates will be in a better position to then lobby for stricter control over the scope of surveillance powers.

Acceptable justification needs to be provided for both the bodies authorized to request surveillance as well as rules on the types of data to be accessed, keeping in mind the fluid and telling nature of what is viewed as transactional data. Finally a trust in the system itself must be regained, with reporting standards that are actionable for aggrieved parties subject to unlawful interception provided for, and a better balance between non-disclosure and fair-access. The continued survival of some of the surveillance legislation in place is questionable, as many are dappled with issues regarding their constitutionality. Thus pro-active and measured engagement with industry, civil society groups and the legislature is essential in charting a coherent and sensible way forward.

11. BIBLIOGRAPHY

PRIMARY SOURCES

Table of cases (SA)

Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC)

S v A 1971 2 SA 293 (T)

S v Naidoo 1998 1 BCLR 46 (D)

Table of cases (FOREIGN)

The United States

Olmstead v United States, 277 US 438, 1928

Katz v. United States 389 US 347 1967

Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., US 1999

United States v New York Telephone Co 434 U.S 159 1977

Smith v. Maryland, 442 U.S. 735 1979

The United Kingdom

Semayne's Case 1604 77 Eng. Rep. 194

Table of statutes (SA)

Constitution of the Republic of South Africa No. 108 of 1996

Electronic Communications Act No. 36 of 2005 as been amended by the Electronic Communications Amendment Act No 37 of 2007

Electronic Communications and Transactions Act No. 25 of 2002

Interception and Monitoring Prohibition Act No. 127 1992

Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 as amended by The Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Act No 48 of 2008

Telecommunications Act No. 103 of 1996 (repealed)

Table of statutes (Foreign)

The United States

Communications Act of 1934

Omnibus Crime Control and Safe Streets Act 1968

Communications Assistance for Law Enforcement Act 1994

Electronic Communications Privacy Act 1986

Foreign Intelligence Surveillance Act 1978

Patriot Act 2001

The United Kingdom

Human Rights Act 1998

Interception of Communications Act 1985

Anti-Terrorism, Crime and Security Act 2001

Communications Act 2003

Treaties and government documents

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The Council of Europe Convention on Cybercrime CETS No: 185, 2001

The Council of Europe Data Retention Directive Regulations 2006

The Council of Europe Data Retention Directive Regulations 2009

The Council of Europe Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The Council of Europe's resolution on the lawful interception of telecommunications

The European Convention on Human Rights 1950

The United States

Committee on the Judiciary's Congressional Hearing 'Fourth Amendment issues raised by the FBI's "Carnivore" Program' transcript available at *http://commdocs.house.gov/committees/judiciary/hju67305.000/hju67305_0f.htm* [Accessed 20 December 2010]

The United Kingdom

The 'Interception of communications in the United Kingdom: A consultation paper' 1999 at 10

South Africa

GN R93 *GG* 31844 of 6 February 2009

GN R92 *GG* 31844 of 6 February 2009

GN R1121*GG* 32759 of 27 November 2009

SECONDARY SOURCES

Journals

Branch, Phillip 'Lawful Interception of the Internet' (2003) 1 1 *Australian Journal of Emerging Technologies and Society* 38

Ajdaharian Lusine 'Knocking down the Knock-and-announce rule: A casenote on Hudson v. Michigan 29' (2007) *Whittier Law Review* 183

Long, William & Quek, Marc 'Personal data privacy protection in an age of globalization: the US-EU safe harbour compromise' 9 (2002) *Journal of European Public Policy* 325

Kitch, Edmund W 'The Limits of the Fourth Amendment' (1968) *The Supreme Court Review* Available at *http://www.jstor.org/stable/3108771* [Accessed 15 June 2011]

Tracy Cohen 'But for the nicety of knocking and requesting a right of entry: Surveillance law and privacy rights in South Africa' (2001) 1 *The Southern African Journal of Information and Communication* available at *http://link.wits.ac.za/journal/j-01-tc.htm* [Accessed 2 January 2011]

Hosein, Ian and Escudero-Pascual, Alberto 'Questioning lawful access to traffic data' (2004) 47 *Association for Computer Machinery* 77

Hosein, Ian 'The collision of regulatory convergence and divergence: updating policies of surveillance and information technology'(2002) 1 2 *The Southern African Journal of Information and Communication*

Landau, Susan 'Security, wiretapping and the Internet' (2005) 3 *IEEE Security and Privacy* 26

Cheng, Fa-Chang & Lai, Wen-Hsing 'An overview of VoIP and p2p copyright and lawful interception issues in the United States and Taiwan' (2010) 7 *Digital Investigation* at 81

Aljaz, Tomaz & Dolenc, Franc & Maloku, Naim 'Legal call interception in next generation networks' (2003) 1 *Telecommunications* 47

Osher, Steven 'Privacy, computers and the Patriot Act: the Fourth Amendment isn't dead, but no one will insure it' (2002) 54 *Florida Law Review* 521

Ringland, Kristina 'The European Union's Data Retention Directive and the United States Data preservation law: Finding the better model' (2009) the Shidler Journal of Law Communication and Technology available at *http://www.lctjournal.washington.edu/vol5/a13Ringland.html* [Accessed 28 July 2011]

Murdoch Watney 'State Surveillance of the internet: Human rights infringement or e-security mechanism' (2007) 1 *International Journal of Electronic Security and Digital Forensics* 47

Jeffrey Yeates 'CALEA and RIPA: the US and the UK responses to wiretapping in an increasingly wireless world' (2001) 12 *Albany Law Journal of Science and Technology* 125

Hornle, Julia 'How to control interception – does the UK strike the right balance?' (2010) 16 *Computer Law and Security Review* 649

Mokoena, Stimela & Zambane, Thokozile 'Sshhh - someone may be listening' (2010) 10 *Without Prejudice* 20

Books

Black, S *Telecommunications law in the internet age* (2002) Morgan Kaufmann, San Francisco, California

Burns, Yvonne *Communications Law* (2009) Butterworths, Durban

Diffie, Whitfield and Landau, Susan *Privacy on the line: The politics of wiretapping and encryption updated and Expanded edition* (2007) Kindle Edition

Rule, James *Privacy in Peril* 2ed (2007) Oxford University Press, New York

Clough, Jonathan *Principles of Cybercrime* (2010) Cambridge University Press, New York

Nazreen Bawa 'The Regulation of Interception and Provision of Communication-Related Information Act' in Lisa Thornton et al (ed) *Telecommunications law in South Africa* (2006) 296-332 Act'

Websites

Boucher, Sarah & Cotler, Edward & Larson, Stephen 'Internet wiretapping and carnivore' 2001 Available at *http://groups.csail.mit.edu/mac/classes/6.805/student-papers/spring01-papers/carnivore.doc* [Accessed 27 December 2010]

TCPIPGuide.com 'Circuit switching and packet switching networks' Available at *http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm* [Accessed 20 December 2010]

IIT Kharagpur 'Module 1 Communications networks' Available at *http://nptel.iitm.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Communication%20network/pdf/1.1%20Lesson%201.pdf[Accessed* 8 August 2010]

Technologies for Conservation and Development'Introduction to Communication Technology' Available at *http://www.t4cd.org/Projects/Current%20Projects/Documents/Training%20Manual%20-%20Communications%20Technologies.doc* [Accessed 27 December 2010]

Unuth, Nadeem 'What is a protocol' available at *http://voip.about.com/od/voipbasics/g/protocoldef.htm* [Accessed 26 May 2011]

Joannes Thuy 'Eurojust coordinates internet telephony investigations' Available *http://www.eurojust.europa.eu/press_releases/2009/20-02-2009.htm* [Accessed 12 December 2010]

Comscore Mobile Mondays 'Top US smartphone platforms' available *http://www.comscoredatamine.com/2011/05/mobile-mondays-top-u-s-smartphone-platforms/* [Accessed 23 July 2011]

Gartner Newsroom 'Gartner says worldwide mobile phone sales grew 35% in third quarter 2010; smartphone sales increases 96%' Available at *http://www.gartner.com/it/page.jsp?id=1466313* [Accessed 23 July 2011]

RIM 'Blackberry Internet Service' Available at *http://docs.blackberry.com/en/smartphone_users/deliverables/20443/BlackBerry_Internet_Service-Feature_and_Technical_Overview--1187001-0914104552-001-3.2-US.pdf* [Accessed 15 June 2011]

The Times of India 'Gmail, Blackberry, Skype can't be banned: Panel' Available *http://timesofindia.indiatimes.com/tech/news/internet/Gmail-BlackBerry-Skype-cant-be-banned-Panel/articleshow/8885870.cms* [Accessed 25 June 2011]

Michael A. Vatis – 'The Council of Europe Convention on Cybercrime' Available at *http://www.cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf* [Accessed 17 June 2011]

ETSI 'Lawful Interception (LI); Handover Interface for the lawful interception of telecommunications traffic' (2007) Available at *http://pda.etsi.org/exchangefolder/es_201671v030101p.pdf* [Accessed 17 November 2010]

IETF 'Mission Statement' Available *http://www.ietf.org/about/mission.html* [Accessed 18 November 2010]

My Hosting Reviews 'What is a network uptime guarantee and why is it important?' Available at *http://myhostingreviews.com/network-uptime-guarantee.htm [Accessed 17 July 2011]*

Electronic Frontier Foundation 'Communications assistance for law enforcement act' Available at *http://w2.eff.org/Privacy/Surveillance/CALEA/?f=summary.html* [Accessed 01 December 2010]

Nakashima, Ellen 'A story of Surveillance' Available at *http://msl1.mit.edu/furdlog/docs/washpost/2007-11-07_washpost_mark_klein_hero.pdf* [Accessed 20 June 2011]

Robert Poe 'Can Skype Keep its Secrets' available at *http://www.voip-news.com/feature/skype-calea-compliance-061206/* [Accessed 26 June 2011]

Congressional Research Service 'Cybercrime: The Council of Europe Convention' available at *http://www.iwar.org.uk/news-archive/crs/10088.pdf* [Accessed 22 July 2011]

Fakhoury, Hanni 'Know your rights' available at *https://www.eff.org/wp/know-your-rights* [Accessed 28 July 2011]

Meyer, David 'Pub "fined £8k" for Wi-Fi copyright infringement' available at *http://www.zdnet.co.uk/news/networking/2009/11/27/pub-fined-8k-for-wi-fi-copyright-infringement-39909136/* [Accessed 27 July 2011]

Williams, Chris 'UK jails schizophrenic for refusal to decrypt files' available at *http://www.theregister.co.uk/2009/11/24/ripa_jfl/page2.html* [Accessed 10 June 2011].

Theses

Cull, Dominic *ISPs in the middle* (unpublished LLM thesis, University of Cape Town, 2004

Ferguson, Steven *The monitoring of e-mail and Internet usage in the South African workplace – The final word* (unpublished LLM thesis, University of Cape Town, 2003)

Montgomery, Patrick W *A study into next generation networks for voice services: History, design and policy implications* (unpublished Master's thesis,

Instituto Superior Tecnico ,2005) available at *http://in3.dem.ist.utl.pt/master/thesis/03files/40thesis.pdf* [Accessed 23 December 2010]