'BUT FOR THE NICETY OF KNOCKING AND REQUESTING A RIGHT OF ENTRY':*

SURVEILLANCE LAW AND PRIVACY RIGHTS IN SOUTH AFRICA

TRACY COHEN
LIKK Centre, Graduate School of Public and Development Management, University of the Witwatersrand.

ABSTRACT

As communications tools expand beyond that of the traditional fixed line telephone, so too do the tools for monitoring those communications. Fuelled by dual needs to protect the privacy rights of individuals, as well as monitor the activities of criminals using the communications networks, governments around the world are toning their surveillance laws in accordance with technological developments and constitutional necessity. In the South African context, the clash of rights inherent in this activity warrants an examination of the continued constitutional status of the Interception and Monitoring Prohibition Act of 1992, in light of recent proposals by the Law Commission to amend its provisions. It is argued that whilst the target of such a law justifies its existence, the reach of its ambit potentially displaces its ongoing constitutional validity.

INTRODUCTION

1998: 'Multiple position intercept stations located globally capture all satellite, microwave, cellular and fibre-optic communications traffic and then process this information through the mammoth computer capabilities of the worlds largest and most effective intelligence agency. The system comprises advanced voice and optical character recognition programmes and seeks out code words or phrases that will prompt the computers to flag the message for recording or transcribing for future analysis. Intelligence analysts at each of the "listening stations" maintain separate keyword lists, known as "dictionaries", to analyse any conversation or document flagged by the system, which is then forwarded to the respective intelligence agency headquarters that requested the intercept.'[1]

This scenario is neither an extract from a science fiction novel by William Gibson[2] nor an Orwellian catechism of a futuristic glimpse into the tyranny of government

---

* Hurt J *S v Madiba & another* 1998 (1) BCLR 38 (D) at 441- J.

BA LLB LLM (Witwatersrand)

I wish to thank Professor Ellison Kahn for useful comments and editorial assistance on the final draft of this paper and Fatima Laher for assistance on the initial draft. I also wish to thank Lisa Forman, Alison Gillwald, Dieter Zinnbauer and Myron Zlotnick for various comments and suggestions on the ideas that inform this paper. The final draft of this paper was written during a research fellowship at the Columbia Institute of Tele-Information (CITI) at Columbia University. This fellowship was made possible by funding provided by the Internet Service Providers' Association (ISPA) of South Africa. I am also grateful for the assistance received at CITI.

[1] Patrick S Poole 'ECHELON: America's Secret Global Surveillance System' *The Privacy Papers* (Washington: Free Congress Research and Education Foundation 1998).

[2] William Gibson coined the term 'Cyberspace' in his 1984 novel *Neuromancer 51.*

empowered by technology. It describes an actual, global surveillance system operating today. Codename: ECHELON. Created by the United States National Security Agency (NSA), ECHELON is a vast network of electronic spy stations located around the world and maintained in conjunction with security agencies in the United Kingdom, Canada, Australia and New Zealand.[3] These countries, bound together in a still-secret agreement dating back to 1948 called UKUSA, allegedly intercept and gather electronic signals of almost every telephone call, fax transmission and e-mail message transmitted around the world daily. The official targets of ECHELON are the communications inherent in political spying and commercial espionage. The reach of ECHELON, however, extends to the personal, political, religious and commercial communications of citizens.[4]

The surveillance of electronic communications or 'wiretapping' is conducted in nearly every country in the world by governments. Despite a number of procedural safeguards, it is frequently abused.[5] Although not limited to it, the most renowned target of the wiretap is the standard fixed-line telephone system.[6] A rudimentary wiretap, undetectable to the target, can be placed in a variety of locations and requires little skill and inexpensive technology to operate.[7] Despite varying approaches to privacy, this activity is sanctioned by laws passed under all forms of government.

This paper provides an overview of the existing Interception and Monitoring Prohibition Act[8] ('the Act') in South Africa, with particular reference to telephone calls.[9] The primary object of this paper is to assess the extent of judicial synergy between the surveillance laws and privacy rights.[10] Following an analysis of the history and operation of the Act, it is conceded that the prohibition as enacted in 1993 is on the face of it constitutional. However, it is asserted that legal, political and technological developments

---

[3] The British General Communications Headquarters, the Canadian Communications Security Establishment, the Australian Defence Security Directorate and the New Zealand General Communications Security Bureau. The first acknowledgement by a government entity of the existence of ECHELON was in an European Union Parliament working report entitled 'An Appraisal of Technologies of Political Control' presented on the 16 September 1998 to the European Parliament. Largely however, government officials repeatedly deny its existence.

[4] Numerous documented cases in the United Kingdom reveal that British intelligence services monitor social activists, labour unions and civil-liberty groups. See 'Bug Off! A Primer for Human Rights Groups on Wiretapping' (Washington: Electronic Privacy Information Centre 1995); Mark Fineman 'Latest Mexico Wiretap Scandal Spurs Move to Curb Widespread Practice' *LA Times* 17 June 1995. For a survey of wiretapping in the UK, see Patrick Fitzgerald & Mark Leopold *Stranger on the Line: The Secret History of Phone Tapping* (London: Bodley Head 1987). For an overview of Australian surveillance law, see 'Guidelines on Voice Monitoring or Recording of Telephone Services' (1994) 1 *PLPR* 55.

[5] In 1995, 200 000 illegal wiretaps were estimated to be in place in Mexico. Litigation in the US under the Freedom of Information Act revealed FBI involvement in monitoring computer networks used by political and advocacy groups. French counter-intelligence agents allegedly monitored telephones of prominent journalists and opposition party leaders during the 1980's. See US Department of State *Country Reports on Human Rights Practices*, (1994).

[6] It should be noted that 'communication' also encompasses 'correspondence', which is much narrower in scope. A distinction also exists with that of 'surveillance', which is usually taken to have application to any form of electronic communication, including computers, newer technologies and networks. For the purposes of this paper, the distinction is not relevant. The term 'surveillance' will be used interchangeably to refer to the range of activities encompassed in monitoring and/or intercepting all electronic forms of communication, written and oral. Transactional information recorded when a call is placed is also capable of being monitored and can provide critical information on sources and the location of people at any given time. See Gregory Millman 'From Dragnet to Drift Net: Telephone Record Surveillance and the Press' *New York Times* 6 September 1980.

[7] For example, microphones in old telephone handsets can be replaced with ones that can transmit to a remote receiver. 'Taps' can be placed in telephone boxes in buildings, in homes, on outside lines or on the telephone pole boxes near the target of surveillance. See 'Bug Off!' op cit note 4 above.

[8] Act 127 of 1992. It should be noted that the Act also provides for the interception and monitoring of postal communications.

[9] A telecommunication line is defined in the Telecommunications Act 103 of 1996 as 'any apparatus, instrument, pole, mast, wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with the sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information'.

[10] As entrenched by s 14 of the Constitution of the Republic of South Africa, Act 108 of 1996.

cast serious doubt on the long-term ability of this law to withstand constitutional muster. It is argued that whilst the target of the legislation operates in a constitutionally acceptable paradigm, the reach of the legislation displaces it. This assertion is contextualised through a brief review of the main proposals by the South African Law Commission (SALC) to amend the present surveillance law to take account of technological developments.[11]

HISTORY OF INTERCEPTION AND MONITORING IN SOUTH AFRICA

The genesis of surveillance laws in South Africa lies in the National Party's self-preservationist obsession with 'security legislation'. The interception of postal articles and telephonic communications was originally authorized in terms of s 118A of the Post Office Act.[12] Advances in technology made it increasingly possible for the unauthorised interception and monitoring of postal articles or telecommunications to take place by both state and private parties. The government, moving for the passage of the Interception and Monitoring Prohibition Bill in 1992,[13] argued that such legislation was necessary in order to protect the individual's common-law right to privacy. To attain this end, the legislation introduced two modifications: First, the Act altered the government functionary who could authorize such interceptions. Section 118A of the Post Office Act granted a government minister the right to exercise that power.[14] In terms of s 2(2) of the Interception and Monitoring Prohibition Act 1992, only a judge or designated retired judge of the Supreme Court [sic] may issue a direction to monitor communications.[15] This change was vital in order to divest the 'security establishment of the state' of the vast powers of authorisation in this regard.[16] The second change necessitated a shift in focus from state security to the combating of serious crime.[17] It was argued that a limitation on the right to privacy for this objective is as legitimate as one in the national interest, especially where syndicates and complex smuggling networks are concerned.[18]

---

[11] Discussion Paper 78 Project 105 *Review of Security Legislation* November 1998.

[12] Act 44 of 1958. The 1972 Potgieter Commission, set up to investigate matters relating to the security of the state, recommended the insertion of s 118A into the Post Office Act. This amendment was seen to accord with similar legislation and powers in Australia, West Germany and Britain. In 1981, the Rabie Commission of Inquiry into security legislation reviewed the provisions of s 118A and proposed certain further administrative, procedural and technical amendments.

[13] Second Reading Debate 17 June 1992 *Hansard* Col 11522. Now the Interception and Monitoring Prohibition Act 127 of 1992.

[14] Under s 118A and 118(2)(b) of the Post Office Act, the Minister of Posts and Telegraphs or any Minister who was a member of the State Security Council could authorize communications interception 'in the interests of state security'.

[15] The SALC has proposed that this be limited to any High Court judge.

[16] *Hansard* op cit note 13 at Col 11523-4. In the administration of justice by the European Court of Human Rights, it was indicated that a judge as the party granting approval was preferable in principle, as judicial authority provided the best guarantee of independence and impartiality.

[17] As defined in Schedule 1 of the Criminal Procedure Act 51 of 1977.

[18] The intention to combat the source and planning of crime is clearly evident in the transcripts of the parliamentary debates. The House of Assembly was divided 104: 34 in favour of the Bill.

THE INTERCEPTION AND MONITORING PROHIBITION ACT

The Interception and Monitoring Prohibition Act[19] repealed s118A of the Post Office Act and came into effect on 1 February 1993, prior to the coming into effect of the interim Constitution.[20] Its purpose is to prohibit the interception and monitoring of certain communications, except in accordance with the law and to provide for authorisation to do so in certain circumstances.[21] A direction to monitor or intercept any communication may be issued on two grounds: if on the presentation of evidence, the judge is convinced that the offence committed or about to be committed is a serious offence that cannot be properly investigated in any other manner, or that the security of the Republic is threatened.[22] 'Serious offence' is qualified in so far as it must have been committed over a lengthy period of time, on an organised and regular basis; or it must be one that may harm the economy of the Republic, or is an offence contemplated in the Drugs and Drug Trafficking Act 1992.[23]

Although 'national security' is a traditional basis upon which to limit the application of fundamental rights, the lack of definitive content to the concept is cause for concern. The potential 'overbreadth' in this regard may well justify judicial review to determine whether it accords with emergent limitations jurisprudence and can be regarded as 'reasonable and justifiable' in an open and democratic society.[24] The Act stipulates the manner and procedure of applications for directions[25] and contains a 'secrecy' provision preventing any person authorized to perform functions under the Act from improperly disclosing any information.[26] Offences and penalties are provided for in cases where the secrecy provisions or the blanket prohibition on unlawful monitoring and interception are violated.[27]

Given South Africa's history of state policing methods, the legislature had sufficient presence of mind to fortify the constitutional foundations of this Act with a number of substantive and procedural safeguards. Noting the practices of the apartheid regime, the courts have also stressed the importance of due process. Violations in this regard will automatically vitiate the direction and not only constitute a criminal offence in terms of s

---

[19] Act 127 of 1992, as amended by the Intelligence Services Act 38 of 1994, which came into effect on 1 January 1995 and the Interception and Monitoring Prohibition Amendment Act 77 of 1995, as amended by the Judicial Matters Amendment Act 34 of 1998.

[20] Constitution of the Republic of South Africa Act 200 of 1993, which came into operation on 27 April 1994.

[21] See s 2(1) and 2(2)*(c)* respectively. The Act prohibits any person from intentionally intercepting a communication, which has been or is being transmitted by telephone or in any other manner over a telephone line. It further prohibits any person from intentionally monitoring a conversation by means of a monitoring device so as to gather confidential information concerning any person, body or organisation. 'Monitoring' is defined as including the recording of conversations by means of a monitoring device.

[22] Section 3(1)*(b)*(i) and (ii).

[23] Act 140 of 1992, ss 13*(f)* and 14*(b)*.

[24] As required by s 36(1) of the 1996 Constitution.

[25] Section 6.

[26] 'Proper' disclosure implies circumstances where a duty to disclose is supported by the law of evidence or by a competent authority which requires it for the institution or investigation of any criminal prosecution. See s 7(1) *(a) –(d)*.

[27] Section 8 prescribes a fine or imprisonment for a period not exceeding two years for violating s 2 and in the case of a s 7 'secrecy clause' contravention, a fine or imprisonment not exceeding five years.

privacy; and whether the manner in which the evidence was obtained affects its admissibility. Consideration of the latter is not within the scope of this paper.[44]

As regards the first issue, violations of private communication have long been recognised as invasions of privacy in South African law. In *S v A* [45] the court held that eavesdropping and electronic surveillance by private detectives during matrimonial disputes might result in a criminal invasion of privacy if the methods used are unreasonable. The 1998 judgment of *S v Naidoo & another*[46] echoed sentiments expressed in foreign courts, that while surveillance may be necessary in order to facilitate effective police work, it may only be carried out pursuant to a judicial authority. Any monitoring that occurs without such authority is a contravention of the law and a violation of the constitutional right to privacy. Cases pursuant to *Naidoo* have shared the view that only an 'overriding justification of public interest' could prevail against the unlawful manner in which information was obtained and the infringement on the right to privacy that ensues.[47] However, the exact content given to the vague notion of 'public interest' remains imprecise.[48] A middle-ground approach was articulated in *Protea*[49] where it was stated that whether a constitutional right should prevail with unmitigated force would have to depend on the merits of the case and a discretion exercised with due regard to s 36(1), the limitations clause. Invariably, this involves a balancing act, weighing up the competing interests of uncovering the truth (which is always in the public interest) with the interests of protecting the right to privacy.

QUESTIONING CONSTITUTIONALITY?

> 'He took a twenty-five cent piece out of his pocket. There, too, in tiny clear lettering, the same slogans were inscribed and on the other face of the coin the head of Big Brother. Even from the coin the eyes pursued you. On coins, on stamps, on the covers of books, on banners, on posters and on the wrappings of a cigarette packet – everywhere. Always the eyes watching you and the voice enveloping you. Asleep or awake, working or eating, indoors or out of doors, in the bath or in bed – no escape. Nothing was your own except the few cubic centimeters inside your skull.'[50]

Despite a growing need for privacy protection in the information age, it is naïve to assume that procedurally competent surveillance legislation is likely today to be unconstitutional. It is also arguable that technology is developing to such a degree that the ability of governments to monitor and intercept private communications, however well

---

[44] The central issue in this regard is the extent to which – if at all - the common law governing admissibility has been superseded by s 35(5) of the Constitution. Section 35(5) provides that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice. See *S v Motloutsi* 1996 (2) BCLR 220 (C); *S v Naidoo & another* 1998 (1) BCLR 46 (D); *Lenco Holdings Ltd & others v Eckstein & others* 1996 (2) SA (A) 693 and *Protea Technology Ltd* 1997 (9) BCLR 1225 (W). But see also *Goosen v Caroline's Frozen Yoghurt Parlour (Pty) Ltd & another* 1995 (2) BCLR 68 (IC). The SALC proposals attempt to place the matter beyond doubt. It proposes that information regarding crime, obtained through any interception or monitoring in terms of the Act, or any similar Act in another country may be admissible as evidence in criminal proceedings.

[45] 1971 (2) SA 293 (T). In this case, private detectives were convicted on charges of *crimen injuria* for installing a 'transmitter wireless microphone' under the complainant's dressing table at the request of an estranged spouse.

[46] 1998 (1) BCLR 46 (D). Here the court had to consider the admissibility of evidence in criminal proceedings obtained via an unlawfully monitored conversation.

[47] See, for example, *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A).

[48] In *Financial Mail*, two important ratios emerged: first, that there is a wide difference between what is interesting to the public and what is in the public interest and second, that there is a public interest of a high order in preserving confidentiality in regard to private affairs. See at 462E.

[49] 1997 (9) BCLR 1225 (W).

[50] George Orwell, *Nineteen Eighty-Four* (Penguin Books: 1954) *p* 25.

intentioned, may one-day render the operation of such legislation questionable. It is the aim of this section to consider a variety of factors that may cast doubt on the continued status of this law as constitutional. The recent proposal by the SALC is instructive in this regard and will be considered below. [51]

The security of the Republic

A judge may authorise surveillance if a serious offence is about to be or has been committed or if he or she believes that the security of the Republic is threatened or that it is necessary to gather information concerning a threat to the security of the Republic.[52] Arguably, the former of the two cited aims remains an unassailable ground of attack. Given current and growing levels of criminal activity in South Africa, it may be anticipated that limitations on fundamental rights to combat crime will increasingly be viewed as reasonable and justifiable. The latter basis of authority - 'national security'- is not as robust and suffers from vagueness due to a lack of definition.[53]

The concept of 'national security' is generally imprecise and can be applied in a myriad of circumstances to justify a range of government activities.[54] During apartheid, many laws were in force which, on the basis of alleged national-security concerns, limited fundamental rights in various ways.[55] Many of these laws still pepper our statute book. The principles of openness, transparency and accountability remain crucial and form part of the democratic package for delivery by the post-apartheid government. In South Africa's nascent constitutional democracy, legislation of this genre heralds problems for absolute constitutionality and has to be reconsidered if not very narrowly applied. This is especially true of legislation that uses 'national security' a motivating ground for promulgation. It is trite that all constitutional rights can in appropriate circumstances be limited, but this limitation has to be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. This in turn implies that a limitation on privacy in the name of 'national security' must impose a reciprocal burden on the state to give some definitive content to those words. A proper analysis of the relationship between legislation authorising surveillance of communications and the interests of national security is complex. To be legitimate, the scope and definition of 'national security' need to be narrowly framed and complemented with presumptions and rules on the burden and standard of proof that facilitates the balance between state and individual liberty. The European Court of Human Rights supports this view, noting that member states use – or abuse – the concept of national security interests and, where they consider this necessary, distort the meaning and nature of the term. Some clarification of what these concepts

---

[51] See text to note 86 below.

[52] Section 3(b)*(i)* and s 3(b)*(ii)* of the Interception and Monitoring Prohibition Act 1992.

[53] Similar provisions exist in other jurisdictions. The UK Interception of Communications Act allows the Home Secretary and the Scottish Secretary to approve intercepts in the interest of national security ; to prevent or detect serious crime and to safeguard the 'economic well being of the UK'. See Martin Hickman Report for Parliamentary Staff *PA News* 24 July 1998.

[54] Fidelis Edge Kanyongolo 'National Security and the Legal Protection of Media Freedom' in *Media Law and Practice* (London: Article 19 1996).

[55] For example, the Defence Act 44 of 1957; the Internal Security Act 74 of 1982; the National Key Points Act 102 of 1980 and the Armaments Development and Production Act 57 of 1968.

the South African situation.[66] This assertion is buttressed by s 14(a) and (b), which prohibit a violation of person, home or property. John Locke pronounced as the famous transcendental idea that 'every man has a "property" in his own person'.[67] That is, all that man (sic) makes and becomes is part of 'his own person' and this nobody has any right to other than himself.[68] This sentiment has been echoed throughout the years by courts saying around the world, that 'the most comprehensive of rights and the right most valued by civilized men is the right to be let alone.'[69] It therefore appears that s 14 of the Constitution as read to pertain to surveillance laws sets an inordinately high standard for limitations review, especially in the light of the specific guarantee in s 14 to privacy of communications.

Target versus reach

An inherent flaw with surveillance legislation is that it fails to discriminate sufficiently between communications warranting interception and those not warranting it. 'There is thus an encroachment on other people's privacy and not only that of the person that one actually wants to bring to book.'[70] This problem of 'target versus reach' of law is not limited to this type of legislation. It is a problem common to legislation that encroaches, albeit justifiably, on a fundamental constitutional right, such as censorship legislation.

Whilst the *target* of the law may be individuals suspected of committing serious offences, or posing a threat to the national security, the *reach* of the legislation may potentially extend to include journalists, human-rights organisations, political dissidents and opposition, as well as innocent individuals living in close proximity to those being monitored, for example families.

In this regard, the Swiss case of *Kopp*[71] is instructive. The European Court of Human Rights found that the Swiss government's tapping of an employee's line in a law firm constituted a breach of art 8, which guaranteed the right to privacy.[72] Noted as the worst of the violations was that the law firm's partners and employees, clients and third parties who had no connection with the criminal proceedings were all monitored. 'This exceeds the bounds of what is required to protect democratic institutions and amounts to a perverse inquisition.' This concern was enunciated in the famous words of Justice Brandeis in *Olmstead v United States*:

---

[65] 389 US 347 (1967).

[66] On search and seizure generally, see Neethling *et al. Law of Personality* (1996) and McQuoid Mason op cit note 31 above. For an interpretation of the scope of the right to privacy and its limitations regarding search and seizure, see the comments of Sachs J in *Ashok Rama Mistry v The Interim National Medical and Dental Council of SA* CCT 13/97 at para 23.

[67] John Locke *The Second Treatise of Civil Government* (1690) (Everyman edition 1924) 129, cited in M R Konovitz 'Privacy and the Law: A Philosophical Prelude' (1966) 31 *Law & Contemporary Problems* 272 at 275.

[68] Quoted in McQuoid-Mason *The Law of Privacy in South Africa* op cit note 31 at 3.

[69] *Olmstead v United States* 277 US 438 (1928) at 478, per Brandeis J.

[70] PC de Jager, MP, made this point during the parliamentary debates on the Interception and Monitoring Bill. He noted '[that] what makes this [Bill] even more unacceptable is that it is not only the suspect's telephone conversations which may be monitored, but also those of his wife and daughter, even when she is talking to her fiancé.' (Sic)

[71] *Kopp v Switzerland* op cit note 56 above. See also the EC Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (96/C 329/01).

[72] The case involved the illegal wiretapping of a lawyer's office telephone on the grounds of national security. The law did not clearly state how, under what conditions and by whom a distinction was to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to other activities. The court held that it was it was wholly unacceptable to assign the task of monitoring to an official of the Post Office's legal department, a member of the executive, without supervision by an independent judge.

'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 wire-tapping.'[73]

Contrary to criminals being thought of as the only targets of such legislative nitiatives, human rights groups, reporters and political opponents are also common argets of surveillance.[74] This need not, however, prompt Orwellian paranoia. There are ractical limitations to surveillance, which is ultimately, a labour-intensive exercise, equiring considerable human resources to conduct taps, listen to and process the ommunications.[75] Cryptographic technology, utilising a mathematical technique for crambling conversations, is also widely available from suppliers of customer premise quipment to 'scramble' calls to ensure that conversations are not easily monitored. For etwork-based communications, such as the Internet, the use of encryption technologies more contentious, especially in so far as their export is concerned.[76] Notwithstanding he availability of technologies to both scramble and unscramble communications, the ssue is less a matter of what is practically possible, than what is judicially desirable. iven the available technology and the convergence of communications, these rotections' do not adequately address the constitutional concerns raised by legislation verbroad in application.

New technology

It appears clear that the Interception and Monitoring Prohibition Act did not nvisage the extent of communications proliferation that technological development is elding. With the exponential annual growth of the Internet, the ability to affect housands more 'communicators' is also increasing and so too are the techniques for nonitoring and interception.[77] The potential target group and thus reach of the legislation re considerably augmented. In addition, serious questions of applicability must be raised bout the ability of the law to keep abreast of technology. Does the Act apply to new echnologies not contemplated at the time of its inception? With the triple effect enerated by deregulation, globalisation and convergence, it is becoming increasingly ifficult to ascertain technological, geographical and legal boundaries. In this context, hat, for example, constitutes a telephone call when a 'normal' voice call can be initiated

277 US 438 (1928) at 475-6.

For example, in the US in 1996 overall 2.2 million conversations were captured via legal interceptions. Prosecutors nsidered 1.7 million intercepted conversations not 'incriminating'. Federal intercepts carried out by the FBI were rticularly inefficient, with only 15.6 percent of the intercepted conversations reported as 'incriminating'. See Comments the Electronic Privacy Information Centre, the Electronic Frontier Foundation and the American Civil Liberties Union fore the Federal Communication Commission, 20 May 1998, on the Communications Assistance for Law Enforcement Act ALEA), 20 May 1998, CC Docket No. 97-213 at 16.

For example, prior to the collapse of the Berlin Wall, the East German police employed 10 000 people to conduct retaps. Comments of Hansjorg Geiger, German Federal Commission for the Stasi Files, April 1994, cited in Banisar op cit te 76 below. Former members of the Soviet KGB recently disclosed that they only had the capability of wiretapping 1000 lephone lines in Moscow and another 1500 for the rest of Russia. See Rafayenko and Rubnikovich 'Total Eavesdropping ppossible' *Russian Press Digest* 8 April 1993.

David Banisar 'US State Department Reports Worldwide Privacy Abuses' *International Privacy Bulletin* Volume 4 No 1 996 at http://www.privacy.org/pi/reports/1995_hranalysis.html

Computer communication has become the main target of surveillance. Providing fast and inexpensive communication with range of applications such as e-mail and voice-over-IP, computers and networks are increasingly targeted for regulation der the guise of security and law enforcement.

from a hand-held computer? Who constitutes a telecommunications carrier? What constitutes an information service?[78] These questions are prompting a new dialogue on efficiencies in regulation in the era of convergence. Trends indicate a move to models based on notions of co-regulation, in an attempt by government to gain assistance from industry for enforcement purposes.[79]

In August 1994, the US Congress passed the Communications Assistance for Law Enforcement Act (CALEA),[80] largely in response to the FBI's concern that new technologies could be used to impede criminal investigations.[81] The object of this enactment, also known as the 'Digital Telephony Act' is to ensure that the government's ability to eavesdrop on rapidly evolving digital services offered by new wired and wireless telecommunications carriers would remain as easy as tapping fixed line phones serviced by local telephone companies.[82] A subsidy fund of 500 million USD was established to ensure that all telephone companies make their networks compliant for this law or risk $10 000 per day in fines.[83] Essentially CALEA requires a redesign of the US communications network to facilitate surveillance on all forms of electronic media.[84]

This law has marked implications for ISPs and Internet telephony firms, as it requires telecommunications companies to wire surveillance technology into their networks which could force Internet telephony firms to configure their systems to be easily wiretapped by law-enforcement agencies. The FCC, whilst trying to decide on how CALEA should apply to Internet telephony, has stated that the law applies to all 'packet-switched technology' that is used to provide telecommunications services. [85] The development and proliferation of new technologies are not in themselves grounds for asserting the unconstitutionality of surveillance laws. However, by the same token the impact of technology means that the ease and extent of global surveillance possibilities give credibility to the potential overbreadth with which such a law may operate.

SOUTH AFRICAN LAW COMMISSION PROPOSALS

In 1998, the South African Law Commission (SALC) began a project to review the existing law on the monitoring and interception of communication and make a number of recommendations for its reform.[86] This section briefly reviews the most far-reaching of the

---

[78] The distinction being relevant at least in US law, as the FCC has ruled that 'information services' as opposed to 'telecommunication services' are not covered by CALEA. There is an interesting anomaly here in that the FCC has also ruled that IP telephony using computers constitutes an 'information service', while phone-to-phone IP telephony however falls into the category of 'telecommunications service'.

[79] See Monroe E Price and Stefaan G Verhulst 'In search of the self: Charting the course of self-regulation on the Internet in a global environment' unpublished paper of the Programme in Comparative Media Law and Policy, University of Oxford.

[80] H.R. 4922.

[81] See Report of EPIC, EFF and ACLU op cit note 74 above.

[82] Bill Frezza 'The CALEA Time Bomb is Still Ticking' *Freewire* at http://pubsys.cmp.com/nc/813/813colfrezza.html

[83] Centre For Democracy and Technology 'FCC launches CALEA Proceedings' 21 April 1998. Needless to say, this legislative development prompted a variety of lawsuits. The Cellular Telephone Industry Association and the Personal Communications Industry association filed a suit in April 1998 against the Department of Justice and the FBI, claiming that CALEA unlawfully shifts the cost of paying for phone equipment upgrades for wiretapping from the FBI to the telephone companies.

[84] Included in this redesign is a call for standards that require every cell phone to provide location information of users to police.

[85] Declan McCullagh 'Wiretapping Internet Phone Lines' *Wired News* 10 November 1998. Many intelligence agencies have also lobbied to limit the security features in GSM in order to facilitate interception of cellular telephony. See Bernard Lagan & Anne Davies 'New Digital Phones On-line Despite Objections' *The Sydney Morning Herald* 28 April 1998.

[86] Discussion Paper 78 Project 105 *Review of Security Legislation* November 1998. The SALC issued a discussion paper, designed to elicit comment as the basis for reform. The document compared domestic surveillance laws with those of France, the Netherlands, Belgium, Germany, Britain, Canada, Hong Kong and the United States and found that it compared

proposals to buttress the assertion that technological developments, coupled with the new intended application of these laws, contribute to questions of constitutionality. The proposals introduce a range of measures that can be clustered into two areas: application of the law and the cost of surveillance. [87]

The main proposal requires that no telecommunication service may be provided which does not have the capacity to be monitored.[88] Existing services lacking surveillance capability will be have to acquire the necessary facilities for it. All costs associated with such surveillance, including investment, technical, maintenance and operating costs, must be carried by the telecommunication-service provider. The proposals create an obligation on service-providers to assist in the surveillance not only of 'conversations' but also of 'communications', which is a much broader notion that encompasses speech, music, data, text and visual images. This would take into account the full range of communication services available on all distribution platforms.

The SALC has also suggested that the definition of 'serious offence' be expanded to include compelling national interests of the Republic in addition to those presently included as serious offences.[89] It has also proposed that the existing proviso that the serious offence has to be committed over a lengthy period of time be deleted and that the 'interests' of the Republic be inserted to expand on the criteria constituting the security of the Republic. This only serves to strengthen assertions of vagueness mentioned above. In line with similar measures in other jurisdictions, the SALC has also proposed that all telecommunications service providers keep 'registers' for both contract and pre-paid customers of their identities and addresses.[90] Panopticon-like in operation, an amendment will require the army, police and national intelligence to establish surveillance centres to lawfully monitor communications. This will be developed at the state's expense, but cost-sharing agreements with industry are not to be excluded. A recent announcement by the British government to build a central system to monitor all the Internet traffic in the United Kingdom estimates that the cost to British Internet service-providers will reach £30 million in the first year. [91] Obviously, there is substantial controversy as to how this cost should be

---

favourably. The origin of the investigation lay in a request from the Minister for Safety and Security to review and rationalise South Africa's security legislation in view of the political changes. The SALC prioritised the investigation into interception and monitoring of communications for crime investigation and intelligence-gathering purposes. The SALC proposals do not extend to hacking or Internet specific legislation, which is the focus of the SALC's investigation into computer-related crimes (Project 108).

[87] The question of cost remains contentious. Telkom and the cellular operators have argued that surveillance of communications is a state function and that the revenue derived from ordinary taxes should be sufficient. The counter-argument is that telecommunications operators are in possession of a very lucrative resource and it is appropriate that they should carry particular obligations. Whilst the matter is not settled, the SALC favours the latter's argument.

[88] The SALC proposes that the term 'capacity' and not 'capability' should be used. It is further proposed that the Minister may specify the security, technical and functional requirements of the facilities and devices to be acquired.

[89] The SALC initially considered making provision in the Bill for the offences contemplated in ss 100 and 101 of the Telecommunications Act 1996 to be serious offences for purposes of the Interception Act. This would mean that the Independent Communications Authority of South Africa (ICASA) (Act 13 of 2000) would be able to lay a charge with and request the South African Police Service (SAPS) to apply for a direction to authorise the interception and monitoring of telecommunications once ICASA inspectors have reasonable grounds to believe that telecommunication- service providers are in breach of the provisions of the Telecommunications Act. It was also suggested that the office of the President should be vested with a similar right regarding all state departments. The SALC, however, decided against this and the categories of bodies that are presently empowered to apply for directions under the Act remain unchanged.

[90] Legislation in France is currently being debated requiring the names of all who publish on the Internet to be registered with the authorities. This law, ironically titled the Liberty of Communication Act, is without precedent in Europe or the United States.

[91] The Government Technical Assistance Centre (GTAC) will be established as part of the Regulation of Investigatory Powers Bill, expected to become law by September 2000. The government will require ISPs, such as Freeserve and AOL, to have 'hardwire' links to the new computer facility in order to trace messages across the Internet. Home Office permission to search for e-mails and Internet traffic will still be required, but the police can apply for general warrants that would enable them to intercept communications for a company or an organisation.

structured and whether it should be shared with the government. At very least, all British ISPs will have to carry the cost of a mandatory connection to the centre through dedicated lines.[92]

The SALC's stated object of amendments to the surveillance law is again the combating of organised crime, terrorism and drug trafficking. On a constitutional level, the proposals do very little to enhance the protection of privacy for either individuals or the service-providers required to assist with surveillance.[93] The proposals in addition suggest that the procedure may be dispensed with if a judge considers any case sufficiently urgent.[94] This flies in the face of both extant case law and the very motivation for the original amendment to the principal Act: the expansion of privacy rights. Arguably, then, the proposals also add strength to the above argument of overbreadth. Through the use of the definition of 'telecommunication service' in the Telecommunications Act, any entity providing a telecommunication service for which a licence is required falls within the ambit of the Act.[95] The proposal to expand the definitions contained in the Act to include all communications and messages, including e-mails, implies that every communications-network system, regardless of size and service, is intended for inclusion. The lack of a 'common carrier' defence in South African law, a legislative inoculation against liability for acts by third parties using a network, where the network could not reasonably have any knowledge of those acts serves to bolster this line of reasoning. Notwithstanding the above, it is likely that, given the current crime rates in the country and the potential applications of technology to crime, surveillance laws will withstand constitutional scrutiny. The need, however, remains to reduce the scope of privacy dilution as much as possible for users and subscribers on the networks. Other concerns regarding the proposals can be clustered into three corresponding areas: that the cost implied places an undue burden on service providers and that this cost will translate ultimately into higher costs for consumers; that the amount of client or subscriber information required by service providers is excessive and may lead to abuse; and that service providers will become *de facto* state auxiliaries. Ultimately, the most delicate act of balancing of rights is required to provide equilibrium between individual rights and state interests.

CONCLUSION

> 'I might have been a goldfish in a glass bowl for all the privacy I got.' [96]

Historically, the shift from primitive communities to modern cities and the creation of the new society have brought with them new threats to privacy. Criminal-investigation

---

[92] Similar cost-sharing agreements were made between the US government and US telecommunications carriers. See http://www.sunday-times.co.uk/news/pages/sti/2000/04/30/stinwenws01034.html

[93] For example, MTN suggested to the SALC that owing to the sensitive nature of the information, service providers be allowed to answer the directions by way of affidavit and that to protect its employees a structure should be created in the event of any judicial proceeding whereby the affidavit will be used in such proceedings and employees will not be required to testify in court.

[94] This may include the granting of an oral direction followed up by written application incorporating the terms of the directive within one week that where an oral direction was issued, a judge must reduce it to writing within two days.

[95] 'Telecommunication service' is defined with reference to 'telecommunication system', which means any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to rearrangement, composition or other processes by any means in the course of transmission or emission or reception. "Telecommunication facility" means any wire, cable, antenna, mast or any other thing, which is or may be used for or in connection with telecommunication.

[96] H H Munro *The Innocence of Reginald* (1904).

techniques have also improved with the development of technology. World War II and technological spin-offs from the Cold War and the post-war period of increasing empirical research by social scientists have added additional impetus. [97] On a sociological level, the notion of the 'social contract' as perceived by Thomas Hobbes has played a contributory role. In *Leviathan*[98] the Hobbesian man lays down his arms and his rights to the sovereign, in order to empower the sovereign completely. This original notion of the 'social contract' has application to modern-day police enforcement, whereby, in order to protect citizens (and privacy), police powers are consensually increased.[99] Over the years, there has been a colossal and universal 'buy-in' to the need for electronic surveillance by government and industry for security reasons, by a collective universal unconscious labouring under the misapprehension that only 'wrongdoers' are scrutinised.[100] Simultaneously, individuals recognise and zealously guard the view that the people next door should not know what goes on in another's home, the inviolable space and that telephone tapping and other invasions of privacy are abhorrent.

Yet, whilst enjoying the exposure of the 'wrong-doer' in the mainstream media, perhaps one of the most dangerous of all threats is the global voyeurism endorsed at all levels. The need for constant sources of accurate and unbiased information has led to twenty-four-hour news channels that allow us to observe war, famine and inhumanity unfold on our screens. As if non-fiction is not sufficient, we recreate it in fiction, in books, movies, cartoons and magazines,[101] and invent fantasy and futuristic stories about global spy networks and international surveillance. In so doing, whilst we exercise another invaluable right, that to freedom of expression and the media and foster the human need for creativity, we indirectly romanticize and endorse the contexts in which surveillance and monitoring takes place. Essentially, we allow the simultaneous criticism and veneration of such practices. Of course, the 'social contract' does not clearly raise the question of from whom the citizen ought to seek protection. What Hobbes could not possibly imagine is that the technological Leviathan may become more powerful than both individuals and the sovereign combined. *Per contra*, the evolution of a critical judicial system separate from the state as a concept allows us the mechanism to ensure that, whilst this situation exists in culture, it is not endorsed in law. Given the spectre of potential abuse and invasion of rights, coupled with impending technological developments, legislation that allows interception and monitoring of communications has to be stringently examined and even more stringently applied, if it is to enjoy an ongoing constitutionally valid status.

---

[97] E Shils 'Privacy: Its Constitution and Vicissitudes' (1966) 31 *Law and Contemporary Problems* 289, cited in McQuoid-Mason *The Law of Privacy in South Africa* op cit note 31 at 6.

[98] 1651.

[99] Timothy Miller 'Law, Privacy and Cyberspace' (1996) 1 (4) *Communications Law* at 144.

[100] In this reasoning, Shils points to the truism that privacy is in conflict with other valued social interests, such as informed and effective government, law enforcement and free dissemination of news. This view also manifests in the conflict between fundamental rights, such as freedom of speech and equality as regards obscenity. The inherent idea remaining is that a clash of rights is inevitable and the judiciary has its greatest challenge in balancing these rights so as to give effect to the intention and spirit of the legislation that came about through democratic process.

[101] Examples here include Spy v Spy cartoons, The Truman Show, The Matrix and the George Orwell classic, *1984*. This is obviously not to negate the importance of constant and accurate information flows, which clearly yield more benefits than disadvantages.